PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-203371

(43)Date of publication of application : 30.07.1999

---

(51)Int.Cl. G06F 19/00

G06K 17/00

G06K 19/10

G07D 9/00

G07F 7/08

G07G 1/12

G07G 1/14

---

(21)Application number : 10-002441 (71)Applicant : NIPPON CONLUX CO LTD

(22)Date of filing : 08.01.1998 (72)Inventor : OTA MICHIHIRO

---

(54) METHOD AND SYSTEM FOR SETTLMENT USING IC CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To maintain anonymity by comparatively simple structure and to perform early detection of dishonesty and transfer distribution of a value by filling the value in a payment card, performing transaction with a seller by a user without identifying oneself, settling the value by the seller by identifying oneself and transferring the value by performing mutual authentication between the payment card and a storage card.

SOLUTION: A settlement system is constituted of a filling terminal 11, a settlement terminal 12, an issued balance management database 13 to be owned by an issuer 1 of the card, the payment card 21 to be owned by the user 2 and the storage card 31 and a transaction terminal !32 to be owned by the seller

3. The value to be a consideration of a product and service, etc., is filled in the payment card 21 by the filling terminal 11 and the value is withdrawn from the storage card 31 by the settlement terminal 12. The balance which is already issued and not withdrawn is stored in the issued balance management database 13. When offering of the product and the service, etc., is received from the seller 3 and the value is paid as the consideration by the user 2, the value is transferred from the payment card 21 to the storage card 31 via the transaction terminal 32.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the settlement-of-accounts approach using the IC card which settles accounts by using the IC card which stored the value information used as goods or the countervalue of service, and moving said value information The restoration terminal which fills up with said value information the 1st IC card which the payment person of said countervalue uses, and this 1st IC card performs mutual recognition. When this mutual recognition is successful, said 1st IC card is filled up with said value information from said restoration terminal.

In case the payment person of said countervalue and the receiver of this countervalue settle accounts, said 1st IC card and the 2nd IC card which said receiver uses perform mutual recognition. When this mutual recognition is successful, said value information is moved to said 2nd IC card from said 1st IC card. The liquidation terminal which liquidates by receiving said value information from said the 2nd IC card and this 2nd IC card performs mutual recognition. The settlement-of-accounts approach using the IC card characterized by liquidating by moving said value information to said liquidation terminal from said 2nd IC card when this mutual recognition is successful.

[Claim 2] Said 2nd IC card is the settlement-of-accounts approach using the IC card according to claim 1 characterized by notifying said owner identification code with migration of this value information when memorizing the owner identification code of a proper to said receiver and making him move said value information to said liquidation terminal.

[Claim 3] Said 1st IC card memorizes the card identity sign of a proper to this 1st IC card. Said restoration terminal When filled up with said value information, the frame and said card identity sign of this value information are made to correspond, and it memorizes in an outstanding-balance-of-issue-amount management database. Said 2nd IC card When receiving said value information from said 1st IC card, this value information is made to correspond with said card

identity sign, and is received. Said liquidation terminal When receiving said value information from said 2nd IC card, while making this value information correspond with said card identity sign and receiving it The frame and this card identity sign of the received this value information are memorized in said outstanding-balance-of-issue-amount management database. Said outstanding-balance-of-issue-amount management database The settlement-of-accounts approach using the IC card according to claim 1 or 2 characterized by comparing the total amount of restoration and the total amount of receipt of said value corresponding to said card identity sign, and detecting a malfeasance based on this comparison result.

[Claim 4] Said restoration terminal gives the issue number of a proper to this value information, when filled up with said value information. The frame and said issue number of this value information are made to correspond, and it memorizes in an outstanding-balance-of-issue-amount management database. Said 2nd IC card When receiving said value information from said 1st IC card, this value information is made to correspond with said issue number, and is received. Said liquidation terminal When receiving said value information from said 2nd IC card, while making this value information correspond with said issue number and receiving it The frame and this issue number of the received this value information are memorized in said outstanding-balance-of-issue-amount

management database. Said outstanding-balance-of-issue-amount management database The settlement-of-accounts approach using the IC card according to claim 1 or 2 characterized by comparing the total amount of restoration and the total amount of receipt of said value corresponding to said issue number, and detecting a malfeasance based on this comparison result.

[Claim 5] Said 1st IC card generates the random number of arbitration, and said mutual recognition transmits the encryption transmit information which compounded the this generated random number to predetermined transmit information, and was enciphered to said 2nd IC card. Said encryption transmit information is decrypted with said 2nd IC card, and is separated with said random number. The random number which decrypted said encryption reply information and separated that a letter was answered as encryption reply information that the separated this random number was compounded and enciphered by predetermined reply information, and said generated random number by carrying out a comparison check Attest said 2nd IC card and said 2nd IC card generates the random number of arbitration. The encryption transmit information which compounded the generated this random number to predetermined transmit information, and was enciphered is transmitted to said 1st IC card. Said encryption transmit information is decrypted with said 1st IC card, and is separated with said random number. The random number which

decrypted said encryption reply information and separated that a letter was answered as encryption reply information that the separated this random number was compounded and enciphered by predetermined reply information, and said generated random number by carrying out a comparison check The settlement-of-accounts approach using the IC card according to claim 1 to 4 characterized by carrying out by attesting said 1st IC card.

[Claim 6] The settlement-of-accounts approach using the IC card according to claim 1 to 5 characterized by constituting said the 1st IC card and said 2nd IC card in the same IC card.

[Claim 7] In the settlement system using the IC card which settles accounts by using the IC card which stored the value information used as goods or the countervalue of service, and moving said value information The 1st IC card which the payment person of said countervalue uses, and the 2nd IC card which the receiver of said countervalue uses, The restoration terminal which fills up said 1st IC card with said value information, and the liquidation terminal which liquidates by receiving said value information from said 2nd IC card, The dealings terminal which mediates the communication link between said 1st IC card and said 2nd IC card, The outstanding-balance-of-issue-amount management database which carries out the storage management of the frame of the value information with which said restoration terminal was filled up, and

the frame of the value information which said liquidation terminal liquidated is provided. Said 1st IC card The 1st mutual recognition means which performs mutual recognition between either of said restoration terminal and said 2nd IC card, The 1st value information migration means to which said value information stored in the 1st value information storing means is moved is provided. the 1st value information storing means which stores said value information -- this -- 2nd mutual recognition means by which said 2nd IC card performs mutual recognition between either of said liquidation terminal and said 1st IC card, The 2nd value information migration means to which said value information stored in the 2nd value information storing means is moved is provided. the 2nd value information storing means which stores said value information -- this -- said restoration terminal The 3rd mutual recognition means which performs mutual recognition between said 1st IC card, A value information restoration means by which it is filled up with said value information, and an amount storage means of restoration to store in said outstanding-balance-of-issue-amount management database the frame of the value information with which this value information restoration means was filled up are provided. 4th mutual recognition means by which said liquidation terminal performs mutual recognition between said 2nd IC card, A value information liquidation means to receive and liquidate said value information, and an adjusted amount storage means to store in said

outstanding-balance-of-issue-amount management database the frame of the value information liquidated by this value information liquidation means are provided. Said dealings terminal is a settlement system using the IC card characterized by providing a notice means of dealings initiation to notify initiation of settlement-of-accounts dealings to said 1st IC card, and a transmission means to mediate the communication link between said 1st IC card and said 2nd IC card.

[Claim 8] Said 2nd IC card is a settlement system using the IC card according to claim 7 characterized by providing further an owner identification code storing means to memorize the owner identification code of a proper to said receiver, and a notice means of an owner identification code to notify said owner identification code to said liquidation terminal with migration of the value information by said 2nd value information migration means when liquidating between said liquidation terminals.

[Claim 9] Said 1st value information migration means possesses the 1st value information addition-and-subtraction means which subtracts and adds value information stored in said 1st value information storing means. The amount of restoration is added to the value information for which said 1st value information addition-and-subtraction means is stored in said 1st value information storing means when receiving restoration of value information from said restoration

terminal. A payment frame is subtracted from the value information for which said 1st value information addition-and-subtraction means is stored in said 1st value information storing means when payment [the value information on said 2nd IC card]. Said 2nd value information migration means possesses the 2nd value information addition-and-subtraction means which subtracts and adds value information stored in said 2nd value information storing means. The amount of receipt is added to the value information for which said 2nd value information addition-and-subtraction means is stored in said 2nd value information storing means when receiving value information from said 1st IC card. The settlement system using the IC card according to claim 7 characterized by subtracting an adjusted amount from the value information for which said 2nd value information addition-and-subtraction means is stored in said 2nd value information storing means when liquidating between said liquidation terminals.

[Claim 10] A card identity sign storing means by which said 1st IC card stores the card identity sign of a proper in this 1st IC card, A notice means of a card identity sign to notify said card identity sign to this restoration terminal when receiving restoration of value information from said restoration terminal is provided further. Said amount storage means of restoration Make the card identity sign notified by the frame of the value information with which said value information restoration

means fills up said 1st IC card, and said notice means of a card identity sign correspond, and it memorizes to said outstanding-balance-of-issue-amount management database. When moving said value information, said 1st value information migration means makes this value information and said card identity sign correspond, and moves. Said 2nd value information migration means When moving said value information, this value information and said card identity sign are made to correspond, and it moves. Said 2nd value information storing means When it stores said value information, this value information and said card identity sign are made to correspond, and it stores. Said adjusted amount storage means The settlement system using the IC card according to claim 7 or 8 with which said adjusted amount storage means is characterized by what the frame and said card identity sign of the value information liquidated between said 2nd IC card are made to correspond, and is memorized to said outstanding-balance-of-issue-amount management database.

[Claim 11] Said value information restoration means possesses further an issue number generation means to generate the issue number of a proper to this value information when filled up with said value information. Said amount storage means of restoration Make the frame of the value information with which said value information restoration means fills up said 1st IC card, and the issue number generated by said issue number generation means correspond, and it

memorizes to said outstanding-balance-of-issue-amount management database. When moving said value information, said 1st value information migration means makes this value information and said issue number correspond, and moves. Said 1st value information storing means When it stores said value information, this value information and said issue number are made to correspond, and it stores. Said 2nd value information migration means When moving said value information, this value information and said issue number are made to correspond, and it moves. Said 2nd value information storing means When it stores said value information, this value information and said issue number are made to correspond, and it stores. Said adjusted amount storage means The settlement system using the IC card according to claim 7 or 8 with which said adjusted amount storage means is characterized by what the frame and said issue number of the value information liquidated between said 2nd IC card are made to correspond, and is memorized to said outstanding-balance-of-issue-amount management database.

[Claim 12] Said 1st mutual recognition means, said 2nd mutual recognition means, said 3rd mutual recognition means, and said 4th mutual recognition means A synthetic means to compound a random-number-generation means to generate the random number of arbitration, and the random number which this random-number-generation means generated and predetermined information,

An encryption means to encipher the output of this synthetic means, and a decryption means to decrypt the enciphered receipt information, While providing further a separation means to divide into predetermined information and a predetermined random number the information decrypted by this decryption means, compounding the random number which said random-number-generation means generated with information predetermined with said synthetic means and enciphering and transmitting with said encryption means That said random number decrypted and separated was compounded and enciphered at this transmission place by the reply information over said predetermined information Said comparison means compares the random number which decrypted the enciphered this reply information with said decryption means, and was separated with said separation means, and the random number which said random-number-generation means generated. The settlement system using the IC card according to claim 7 to 11 characterized by attesting with it being the just communications partner in which said transmission place has the same cryptographic key when the random number separated with said separation means and the random number which said random-number-generation means generated are the same as a result of this comparison.

[Claim 13] The settlement system using the IC card according to claim 7 to 12

characterized by constituting said the 1st IC card and said 2nd IC card in the same IC card.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] About the settlement-of-accounts approach and system which used the IC card, especially, this invention is a comparatively simple configuration, maintains anonymity and relates to the settlement-of-accounts approach and system using the IC card which can perform unjust early detection and **** circulation of value.

[0002]

[Description of the Prior Art] The settlement system which settles accounts using an IC card can be classified into settlement of the value base, and settlement of the trust base. Settlement of the value base is settled by the settlement of accounts by cash being filled up with near in comparison, and the IC card being filled up with value, and moving the value. Settlement of the trust base performs an acknowledgement action based on the individual humanity news recorded on

the IC card, and settles it by online account transfer of fund so that it may be represented by the settlement system using a credit card.

[0003] Moreover, settlement of the value base can be classified into a cash mold and a prepayment mold from the portable type voice of the value.

[0004] In a cash mold, the value received by dealings can be used for payment of another dealings like a transaction with cash. For this reason, although not pursued, it is difficult to discover it what kind of dealings anonymity, i.e., who, conducted in the cash mold where, when forged value is mixed, in order that value may carry out **** circulation.

[0005] In a prepayment mold, once the value with which the issue origin of value filled up the IC card is dealt with, when it is surely the issue origin of value, and it liquidates, that is, goods are purchased, the value will be extinguished in exchange for goods (use impossible other than liquidation). Moreover, a personal identification number is needed in many cases at the time of use. For this reason, to injustice, such as mixing of forged value, although it is a firm system, there is no anonymity and convenience will also be missing.

[0006] Thus, although there are the advantage and demerit in a cash mold and a prepayment mold, respectively, recently, the settlement system which has the advantage of a cash mold and a prepayment mold is also proposed.

[0007] Although anonymity is maintained, when injustice is performed, this

settlement system is a system which can perform a fixed trace, for example, is a system which consists of a registration agency, and the issue engine and financial institution other than the user of an IC card.

[0008] The registration agency registers by making into a pair the identifier of the public key (cryptographic key to which it is the cryptographic key which makes and uses a private key and a pair, and only a user can know a private key) which a user uses, and a user, and guarantees the justification of this public key to a third person. Moreover, this public key is combined with the digital signature of a registration agency, and is stored in an IC card as a registration document.

[0009] Although an issue engine performs issue of value, management, and unjust detection, a user does not reveal an identifier to an issue engine, but since worth of an IC card can be filled up with using a public key for the origin of a guarantee of a registration agency as the substitute of an identifier, i.e., a kana, anonymity is maintainable.

[0010] Although a financial institution manages a user's account and a written request required for restoration of worth of the IC card in an issue engine is published based on a user's request, a written request can be published without a user's kana being known by the financial institution using the technique of [that a user's kana (public key) and real name are not in agreement] a blind signature.

[0011] Here, circulation of the value which the issue engine published is explained. Drawing 11 is drawing having shown the gestalt of the value stored in the IC card in a circulation process.

[0012] Drawing 11 (a) shows the value which the issue engine published to User A (kana aaa), and the face value 1012 (10000 yen) of the value, an identification number 1013 (xxxxx: a thing like the bill number given to the bill) and the kana 1014 (aaa) of an issue place, and an issue engine's digital signature 1015 are given to value 1011.

[0013] When User A payment [User / a part] or transfers all or a part of this value 1011 to User B (kana bbb) as a countervalue, as shown in drawing 11 (b), a transfer certificate is attached to value 1011, and it payment or transfers.

[0014] The face value 1022 (4500 yen) which transfers the transfer certificate 1021 shown in drawing 11 (b) besides value 1011, the transfer certificate number 1023 (yyyyy), the kana 1024 (bbb) of a transfer place, and the signature 1025 (aaa) of User A are attached. The signature 1025 is performed by enciphering value 1011, face value 1022, the transfer certificate number 1023, and a kana 1024 with a private key [that User A knows (**)], and User B can verify it by decrypting with the public key (aaa used as a kana) currently exhibited. Moreover, it is determined on the responsibility by the side of reception (user B) that the same number will not produce the transfer certificate

number 1023.

[0015] Although User A can also perform transfer of value 1011 to other users etc., it cannot be overemphasized that total of the face value of the transferred value cannot exceed face value 1012 (10000 yen) (based on control of the IC card which User A owns).

[0016] Similarly, when User B performs transfer of value etc. to User C (kana ccc), the transfer certificate 1031 is further attached to the transfer certificate 1021 which includes value 1011 as shown in drawing 11 (c), and transfer etc. is performed. The face value 1032 (2100 yen) which transfers the transfer certificate 1031 shown in drawing 11 (c) besides the transfer certificate 1021, the transfer certificate number 1033 (zzzzz), the kana 1034 (ccc) of a transfer place, and the signature 1035 (bbb) of User B are attached. This signature 1035 is also performed using the private key which User B knows similarly.

[0017] Thus, value 1011 can be divided and transferred at the face value of arbitration, and circulates with **** by the chain of a transfer certificate.

[0018] By the way, even if injustice arises in process of circulation of this value 1011, finally it can discover in the case of liquidation (recovery of value) with an issue engine. For example, suppose that the value 1011 (transfer certificate 1021) that User B received transfer from User A was copied, and it used repeatedly. In this case, what User B can use is only the transfer certificate 1021

by which the transfer place was specified as itself (even if it is going to extract and copy value 1011, the side transferred since assignment of an issue place is aaa refuses reception), and since it is enciphered by the signature 1025, the transfer certificate 1021 cannot rewrite the transfer certificate number 1023. Therefore, if it becomes [that the same transfer certificate number is attached with as, and] and these are used even if it copies the transfer certificate 1021, it is specified that the person who performed injustice based on the transfer certificate number in the issue engine is User B. If an issue engine can specify that User B performed injustice, he can ask a registration agency, and he can acquire and expose User's B real name.

[0019]

[Problem(s) to be Solved by the Invention] However, in the settlement system which has the advantage of an above-mentioned cash mold and a prepayment mold, when injustice is performed, the time amount taken to discover this injustice is long, and when injustice is performed based on a stolen card, a trace becomes almost impossible.

[0020] Moreover, in each IC card which a user uses, since a lot of memory and computation time were needed, there was a trouble that cost became high.

[0021] Then, this invention aims at offering the settlement-of-accounts approach and system using the IC card which a comb and a trace are already possible and

can realize discovery when there is injustice with a configuration with high comparatively simple convenience, maintaining anonymity.

[0022]

[Means for Solving the Problem] In order to attain the purpose mentioned above, in invention of claim 1 In the settlement-of-accounts approach using the IC card which settles accounts by using the IC card which stored the value information used as goods or the countervalue of service, and moving said value information The restoration terminal which fills up with said value information the 1st IC card which the payment person of said countervalue uses, and this 1st IC card performs mutual recognition. When this mutual recognition is successful, said 1st IC card is filled up with said value information from said restoration terminal. In case the payment person of said countervalue and the receiver of this countervalue settle accounts, said 1st IC card and the 2nd IC card which said receiver uses perform mutual recognition. When this mutual recognition is successful, said value information is moved to said 2nd IC card from said 1st IC card. When the liquidation terminal which liquidates by receiving said value information from said the 2nd IC card and this 2nd IC card performs mutual recognition and this mutual recognition is successful, it is characterized by liquidating by moving said value information to said liquidation terminal from said 2nd IC card.

[0023] Moreover, in invention of claim 2, in invention of claim 1, said 2nd IC card is characterized by notifying said owner identification code with migration of this value information, when memorizing the owner identification code of a proper to said receiver and making him move said value information to said liquidation terminal.

[0024] In invention of claim 3, it sets to invention of claims 1 or 2. Moreover, said 1st IC card The card identity sign of a proper is memorized to this 1st IC card. Said restoration terminal When filled up with said value information, the frame and said card identity sign of this value information are made to correspond, and it memorizes in an outstanding-balance-of-issue-amount management database. Said 2nd IC card When receiving said value information from said 1st IC card, this value information is made to correspond with said card identity sign, and is received. Said liquidation terminal When receiving said value information from said 2nd IC card, while making this value information correspond with said card identity sign and receiving it The frame and this card identity sign of the received this value information are memorized in said outstanding-balance-of-issue-amount management database, said outstanding-balance-of-issue-amount management database compares the total amount of restoration and the total amount of receipt of said value corresponding to said card identity sign, and it is characterized by detecting a malfeasance

based on this comparison result.

[0025] In invention of claim 4, it sets to invention of claims 1 or 2. Moreover, said restoration terminal When filled up with said value information, the issue number of a proper is given to this value information, and the frame and said issue number of this value information are made to correspond, and it memorizes in an outstanding-balance-of-issue-amount management database. Said 2nd IC card When receiving said value information from said 1st IC card, this value information is made to correspond with said issue number, and is received. Said liquidation terminal When receiving said value information from said 2nd IC card, while making this value information correspond with said issue number and receiving it The frame and this issue number of the received this value information are memorized in said outstanding-balance-of-issue-amount management database, said outstanding-balance-of-issue-amount management database compares the total amount of restoration and the total amount of receipt of said value corresponding to said issue number, and it is characterized by detecting a malfeasance based on this comparison result.

[0026] In invention of claim 5, it sets to invention of claim 1 thru/or either of 4. Moreover, said mutual recognition Said 1st IC card generates the random number of arbitration, and the encryption transmit information which compounded the this generated random number to predetermined transmit

information, and was enciphered is transmitted to said 2nd IC card. Said encryption transmit information is decrypted with said 2nd IC card, and is separated with said random number. By checking by comparing the random number which decrypted said encryption reply information and separated that a letter was answered as encryption reply information that the separated this random number was compounded and enciphered by predetermined reply information with said generated random number Attest said 2nd IC card and said 2nd IC card generates the random number of arbitration. The encryption transmit information which compounded the generated this random number to predetermined transmit information, and was enciphered is transmitted to said 1st IC card. Said encryption transmit information is decrypted with said 1st IC card, and is separated with said random number. It is characterized by carrying out by attesting said 1st IC card by carrying out the comparison check of the random number which decrypted said encryption reply information and separated that a letter was answered as encryption reply information that the separated this random number was compounded and enciphered by predetermined reply information, and said generated random number.

[0027] Moreover, in invention of claim 6, it is characterized by constituting said the 1st IC card and said 2nd IC card in the same IC card in invention of claim 1 thru/or either of 5.

[0028] Moreover, use the IC card which stored the value information used as goods or the countervalue of service in invention of claim 7, and it sets to the settlement system using the IC card which settles accounts by moving said value information. The 1st IC card which the payment person of said countervalue uses, and the 2nd IC card which the receiver of said countervalue uses, The restoration terminal which fills up said 1st IC card with said value information, and the liquidation terminal which liquidates by receiving said value information from said 2nd IC card, The dealings terminal which mediates the communication link between said 1st IC card and said 2nd IC card, The outstanding-balance-of-issue-amount management database which carries out the storage management of the frame of the value information with which said restoration terminal was filled up, and the frame of the value information which said liquidation terminal liquidated is provided. Said 1st IC card The 1st mutual recognition means which performs mutual recognition between either of said restoration terminal and said 2nd IC card, The 1st value information migration means to which said value information stored in the 1st value information storing means is moved is provided. the 1st value information storing means which stores said value information -- this -- 2nd mutual recognition means by which said 2nd IC card performs mutual recognition between either of said liquidation terminal and said 1st IC card, The 2nd value information migration means to

which said value information stored in the 2nd value information storing means is moved is provided. the 2nd value information storing means which stores said value information -- this -- said restoration terminal The 3rd mutual recognition means which performs mutual recognition between said 1st IC card, A value information restoration means by which it is filled up with said value information, and an amount storage means of restoration to store in said outstanding-balance-of-issue-amount management database the frame of the value information with which this value information restoration means was filled up are provided. 4th mutual recognition means by which said liquidation terminal performs mutual recognition between said 2nd IC card, A value information liquidation means to receive and liquidate said value information, and an adjusted amount storage means to store in said outstanding-balance-of-issue-amount management database the frame of the value information liquidated by this value information liquidation means are provided. Said dealings terminal is characterized by providing a notice means of dealings initiation to notify initiation of settlement-of-accounts dealings to said 1st IC card, and a transmission means to mediate the communication link between said 1st IC card and said 2nd IC card.

[0029] Moreover, in invention of claim 8, said 2nd IC card is characterized by providing further an owner identification code storing means to memorize the

owner identification code of a proper to said receiver, and a notice means of an owner identification code to notify said owner identification code to said liquidation terminal with migration of the value information by said 2nd value information migration means when liquidating between said liquidation terminals in invention of claim 7.

[0030] In invention of claim 9, it sets to invention of claim 7. Moreover, said 1st value information migration means The 1st value information addition-and-subtraction means which subtracts and adds value information stored in said 1st value information storing means is provided. The amount of restoration is added to the value information for which said 1st value information addition-and-subtraction means is stored in said 1st value information storing means when receiving restoration of value information from said restoration terminal. A payment frame is subtracted from the value information for which said 1st value information addition-and-subtraction means is stored in said 1st value information storing means when payment [the value information on said 2nd IC card]. Said 2nd value information migration means possesses the 2nd value information addition-and-subtraction means which subtracts and adds value information stored in said 2nd value information storing means. The amount of receipt is added to the value information for which said 2nd value information addition-and-subtraction means is stored in said 2nd value

information storing means when receiving value information from said 1st IC card. When liquidating between said liquidation terminals, it is characterized by subtracting an adjusted amount from the value information for which said 2nd value information addition-and-subtraction means is stored in said 2nd value information storing means.

[0031] In invention of claim 10, it sets to invention of claims 7 or 8. Moreover, said 1st IC card A card identity sign storing means to store the card identity sign of a proper in this 1st IC card, A notice means of a card identity sign to notify said card identity sign to this restoration terminal when receiving restoration of value information from said restoration terminal is provided further. Said amount storage means of restoration Make the card identity sign notified by the frame of the value information with which said value information restoration means fills up said 1st IC card, and said notice means of a card identity sign correspond, and it memorizes to said outstanding-balance-of-issue-amount management database. When moving said value information, said 1st value information migration means makes this value information and said card identity sign correspond, and moves. Said 2nd value information migration means When moving said value information, this value information and said card identity sign are made to correspond, and it moves. Said 2nd value information storing means When it stores said value information, this value information and said card identity sign

are made to correspond, and it stores. Said adjusted amount storage means Said adjusted amount storage means is characterized by what the frame and said card identity sign of the value information liquidated between said 2nd IC card are made to correspond, and is memorized to said outstanding-balance-of-issue-amount management database.

[0032] In invention of claim 11, it sets to invention of claims 7 or 8. Moreover, said value information restoration means An issue number generation means to generate the issue number of a proper to this value information when filled up with said value information is provided further. Said amount storage means of restoration Make the frame of the value information with which said value information restoration means fills up said 1st IC card, and the issue number generated by said issue number generation means correspond, and it memorizes to said outstanding-balance-of-issue-amount management database. When moving said value information, said 1st value information migration means makes this value information and said issue number correspond, and moves. Said 1st value information storing means When it stores said value information, this value information and said issue number are made to correspond, and it stores. Said 2nd value information migration means When moving said value information, this value information and said issue number are made to correspond, and it moves. Said 2nd value information storing means When it

stores said value information, this value information and said issue number are made to correspond, and it stores. Said adjusted amount storage means Said adjusted amount storage means is characterized by what the frame and said issue number of the value information liquidated between said 2nd IC card are made to correspond, and is memorized to said outstanding-balance-of-issue-amount management database.

[0033] Moreover, in invention of claim 12, it sets to invention of claim 7 thru/or either of 11. Said 1st mutual recognition means, said 2nd mutual recognition means, said 3rd mutual recognition means, and said 4th mutual recognition means A synthetic means to compound a random-number-generation means to generate the random number of arbitration, and the random number which this random-number-generation means generated and predetermined information, An encryption means to encipher the output of this synthetic means, and a decryption means to decrypt the enciphered receipt information, While providing further a separation means to divide into predetermined information and a predetermined random number the information decrypted by this decryption means, compounding the random number which said random-number-generation means generated with information predetermined with said synthetic means and enciphering and transmitting with said encryption means That said random number decrypted and separated was compounded

and enciphered at this transmission place by the reply information over said predetermined information Said comparison means compares the random number which decrypted the enciphered this reply information with said decryption means, and was separated with said separation means, and the random number which said random-number-generation means generated. As a result of this comparison, when the random number separated with said separation means and the random number which said random-number-generation means generated are the same, said transmission place is characterized by attesting with it being the just communications partner which has the same cryptographic key.

[0034] Moreover, in invention of claim 13, it is characterized by constituting said the 1st IC card and said 2nd IC card in the same IC card in invention of claim 7 thru/or either of 12.

[0035]

[Embodiment of the Invention] Hereafter, the settlement-of-accounts approach using the IC card concerning this invention and one example of a system are explained to a detail with reference to an accompanying drawing.

[0036] Drawing 1 is the block diagram showing the system configuration of a settlement system. A settlement system consists of the restoration terminal 11 and the liquidation terminal 12 which the card publisher 1 has, the

outstanding-balance-of-issue-amount management database 13, the debit card 21 which a user 2 has and the receipt card 31 which a vender 3 has, and a dealings terminal 32.

[0037] The restoration terminal 11 fills up a debit card 21 with the value it is valueless to countervalues, such as goods and service, and the liquidation terminal 12 collects value from the receipt card 31. The outstanding-balance-of-issue-amount management database 13 is a database which memorizes the non-collected balance by issue ending.

[0038] In case a user 2 receives offer of goods, service, etc. from a vender 3 and pays value as the countervalue, value is moved to the receipt card 31 from a debit card 21 through the dealings terminal 32.

[0039] Drawing 2 is the block diagram showing the detail of the restoration terminal 11. The restoration terminal 11 possesses the mutual recognition means 111, the value restoration means 112, the ** / receiving means 113, and the outstanding-balance-of-issue-amount management tool 114, and is constituted. The mutual recognition means 111 is a means to attest mutually the debit card 21 connected through ** / receiving means 113, and its justification, and the value restoration means 112 fills up a debit card 21 with value, when a debit card 21 is attested by the mutual recognition means 111. The outstanding-balance-of-issue-amount management tool 114 performs the

reference and updating of the outstanding balance of issue amount of value which are memorized by the outstanding-balance-of-issue-amount management database 13.

[0040] Drawing 3 is the block diagram showing the detail of the liquidation terminal 12. The liquidation terminal 12 possesses the mutual recognition means 121, the value storing means 122, the ** / receiving means 123, and the outstanding-balance-of-issue-amount management tool 124, and is constituted. The mutual recognition means 121 is a means to attest mutually the receipt card 31 connected through ** / receiving means 123, and its justification, and when the receipt card 31 is attested by the mutual recognition means 121, from the receipt card 31, the value storing means 122 receives value and it stores it. The outstanding-balance-of-issue-amount management tool 124 performs the reference and updating of the outstanding balance of issue amount of value which are memorized by the outstanding-balance-of-issue-amount management database 13.

[0041] Drawing 4 is the block diagram showing the detail of a debit card 21. A debit card 21 possesses the mutual recognition means 211, the value addition-and-subtraction means 212, the value storing means 213, the ** / receiving means 214, and the card ID storing means 215, and is constituted. The mutual recognition means 211 is a means to attest mutually the restoration

terminal 11 and the receipt card 31 which are connected through ** / receiving means 214, and its justification. The value addition-and-subtraction means 212 If it will add to the value in which the value with which it fills up from the restoration terminal 11 is stored by the value storing means 213 if the restoration terminal 11 is attested by the mutual recognition means 211, and the receipt card 31 is attested, the value stored in the value storing means 213 will be subtracted according to the amount of dealings. Moreover, the card ID storing means 215 is a means to store the card ID number of a proper in a debit card 21, and a publisher 1 manages value [finishing / issue] by this card ID number.

[0042] Drawing 5 is the block diagram showing the detail of the receipt card 31. The receipt card 31 possesses the mutual recognition means 311, the value addition-and-subtraction means 312, the value storing means 313, the ** / receiving means 314, and the owner ID storing means 315, and is constituted. The mutual recognition means 311 is a means to attest mutually the liquidation terminal 12 and debit card 21 which are connected through ** / receiving means 314, and its justification. The value addition-and-subtraction means 312 if the liquidation terminal 12 is attested by the mutual recognition means 311 -- since, if the value stored in the value storing means 313 is subtracted and delivery and a debit card 21 are attested to the liquidation terminal 12 It adds to the value which receives the value according to the amount of dealings from a debit card

21, and is stored in the value storing means 313. Moreover, the owner ID storing means 315 is a means to store the owner ID number of a proper in the owner of the receipt card 31.

[0043] Drawing 6 is the block diagram showing the detail of the dealings terminal 32. The dealings terminal 32 notifies and ****** initiation of dealings to ** / receiving means 322, and the debit card 21 which are connected with ** / receiving means 321 connected with a debit card 21, and the receipt card 31, possesses the notice means 323 and is constituted. The dealings terminal 32 does not intervene in the data which ** / receiving means 321, and the ** / receiving means 322 send and receive except for the dealings initiation demand which the notice means 323 of dealings initiation generates.

[0044] Here, with reference to drawing 7 , actuation and communication link data flow of the restoration terminal 11 in the case of restoration of value, dealings, and liquidation, the liquidation terminal 12, a debit card 21, the receipt card 31, and the dealings terminal 32 are explained.

[0045] Drawing 7 is drawing having shown each communication link data flow in the case of restoration of value, dealings, and liquidation.

[0046] Drawing 7 (a) is drawing having shown the data flow delivered and received between a debit card 21 and the restoration terminal 11 in the case of value restoration.

[0047] First, a debit card 21 is inserted in the restoration terminal 11, and if ** / receiving means 214 of a debit card 21, and the ** / receiving means 113 of the restoration terminal 11 are connected and the communication link of a debit card 21 and the restoration terminal 11 is attained, a debit card 21 will transmit a restoration demand to the restoration terminal 11 (step 501). At this time, with the mutual recognition means 211 of a debit card 21, a restoration demand is compounded with several 0, and is enciphered, and the random number R1 and the status S1 which this mutual recognition means 211 generated further are added and transmitted.

[0048] The restoration terminal 11 which received the restoration demand receives a restoration demand by performing decryption and separation with several zero, after separating a random number R1 and the status S1 with the mutual recognition means 111 of this restoration terminal 11. Next, although it requires that the restoration terminal 11 should notify the card ID of this debit card to a debit card 21, at this time, said mutual recognition means 111 compounds the random number R1 and the notice demand of ID which were separated previously, and enciphers, and the synthetic information which compounded the random number R2 which said mutual recognition means 111 generated further to this encryption information, and the status S2 is transmitted to a debit card 21 (step 502).

[0049] The debit card 21 which received synthetic information separates a random number R2 and the status S2 from the synthetic information received with the mutual recognition means 211 of this debit card 21, it acquires encryption information, decrypts this encryption information, and divides it into the notice demand of ID, and a random number R1. It attests with said mutual-recognition means 211 being a just restoration terminal with which processing (separation, composition, and encryption of a random number R1) with the just restoration terminal 11 was performed, that is, the restoration terminal 11 has a common cryptographic key with a debit card 21 if the separated random number R1 is compared with the random number R1 generated previously and both are in agreement here, and the processing to the notice demand of ID which received carries out.

[0050] To the notice demand of ID which received, a debit card 21 compounds the card ID stored in the card ID storing means 215 of a debit card 21 with the random number R2 separated with the mutual recognition means 211 of a debit card 21, and enciphers, and it transmits to the restoration terminal 11 as synthetic information which compounded the random number R3 which said mutual recognition means 211 generated further, and the status S3 (step 503).

[0051] The restoration terminal 11 which received synthetic information separates a random number R3 and the status S3 from the synthetic information

received with the mutual recognition means 111 of the restoration terminal 11, it acquires encryption information, decrypts this encryption information, and divides it into Card ID and a random number R2. Said mutual recognition means 111 compares the separated random number R2 with the random number R2 generated previously, and if both are in agreement, the debit card 21 would perform just processing (separation, composition, and encryption of a random number R2), that is, it will perform processing to the card ID it is [card] the just debit card in which it has a cryptographic key with a as common debit card 21 as the restoration terminal 11 and which was attested and received.

[0052] The restoration terminal 11 acquires a restoration limit [as opposed to / with reference to the outstanding-balance-of-issue-amount management database 13 / a debit card 21 in the outstanding-balance-of-issue-amount management tool 114 of the restoration terminal 11] based on the received card ID. This does not restrict the amount of issue of value to one a debit card ID, i.e., 1 card, and when a limit of the amount of issue is unnecessary, it does not need to acquire it.

[0053] Next, although the restoration terminal 11 notifies a restoration limit to a debit card 21 So that compound the random number R3 and restoration limit which were separated also at this time, and it enciphers, and the random number R4 generated further and status S4 may be compounded, it may

transmit (step 504) and the debit card 21 which received this may attest the restoration terminal 11 In the following communication links, both the restoration terminal 11 and the debit card 21 compound the random number divided into transmit information, and encipher. The random number and the status which were furthermore generated are compounded and it transmits, and although mutual recognition processing in which the side which received it attests is performed for every communication link, since the authentication approach is the same, below, the explanation about authentication is omitted.

[0054] Now, the debit card 21 which received the notice of a restoration limit transmits the subtraction demand of the amount of restoration to the restoration terminal 11 in order to receive restoration of value within the limits of the restoration limit (step 505). While the restoration terminal 11 which received the subtraction demand subtracts the value stored in the value restoration means 112 of the restoration terminal 11, the addition demand of the same amount is transmitted to a debit card 21 (step 506), and the outstanding-balance-of-issue-amount management tool 114 of the restoration terminal 11 updates the outstanding-balance-of-issue-amount management database 13.

[0055] The debit card 21 which received the addition demand fills up value with adding the frame of an addition demand to the value that the value

addition-and-subtraction means 212 of a debit card 21 is stored in the value storing means 213, and notifies restoration termination to the restoration terminal 11 (step 507).

[0056] In addition, when the number of the case where authentication goes wrong during a communication link, or the status becomes unseasonable, restoration processing is stopped as what abnormalities produced in the communication link, but in restoration processing, in order to perform addition processing of a debit card 21 after subtraction processing by the restoration terminal 11 side, the published value does not increase unjustly.

[0057] Drawing 7 (b) is drawing having shown the data flow delivered and received between a debit card 21, the dealings terminal 32, and the receipt card 31 in the case of dealings.

[0058] First, a debit card 21 and the receipt card 31 are inserted in the dealings terminal 32. ** / receiving means 214 of a debit card 21, and the ** / receiving means 321 of the dealings terminal 32 are connected. If ** / receiving means 314 of the receipt card 31, and the ** / receiving means 322 of the dealings terminal 32 are connected and the communication link of a debit card 21, the dealings terminal 32 and the receipt card 31, and the dealings terminal 32 is attained, a vender 3 will input the frame of value in which it trades from the input means which the dealings terminal 32 does not illustrate.

[0059] If the frame of value is inputted, the notice means 323 of dealings initiation of the dealings terminal 32 will transmit a dealings initiation demand to a debit card 21 (step 511). In addition, the frame of value in which it trades is contained in this dealings initiation demand.

[0060] Although the debit card 21 which received the dealings initiation demand communicates with the receipt card 31 and value is moved, a communication link is carried out to the following communication links only between a debit card 21 and the receipt card 31, without the dealings terminal 32 intervening. Moreover, since the authentication approach is the same as above-mentioned restoration processing explained although mutually attested for the communication link of every by actuation of the mutual recognition means 211 of a debit card 21, and the mutual recognition means 311 of the receipt card 31 in case it communicates, a debit card 21 and the receipt card 31 omit explanation here.

[0061] Now, the debit card 21 which received the dealings initiation demand transmits a dealings demand to the receipt card 31 (step 512). The card ID of a proper is contained in the debit card 21 stored in the card ID storing means 215 of the frame of value in which it trades in this dealings demand, and a debit card 21.

[0062] Next, the receipt card 31 transmits the subtraction demand according to

the amount of dealings to a debit card 21 (step 513), and in the debit card 21 which received this, while subtracting the value that the value addition-and-subtraction means 212 of a debit card 21 is stored in the value storing means 213, the addition demand according to the amount of subtraction (amount of dealings) is transmitted to the receipt card 31 (step 514).

[0063] With the receipt card 31 which received the addition demand, the amount of dealings demanded by the addition demand is added to the value that the value addition-and-subtraction means 312 of the receipt card 31 is stored in the value storing means 312. At this time, the value to store is made to correspond with the card ID acquired previously, and the value storing means 312 stores it.

[0064] After the processing to an addition demand is completed, the receipt card 31 notifies dealings termination to a debit card 21, and ends migration (dealings) processing of value (step 515).

[0065] Moreover, although the dealings terminal 32 does not intervene in the communication link of a debit card 21 and the receipt card 31, it can know the advance situation of dealings by monitoring the contents of a communication link and acquiring Status Sn.

[0066] Drawing 7 (c) is drawing having shown the data flow delivered and received between the receipt card 31 and the liquidation terminal 12 in the case of value liquidation.

[0067] First, the receipt card 31 is inserted in the liquidation terminal 12, and if ** / receiving means 314 of the receipt card 31, and the ** / receiving means 123 of the liquidation terminal 12 are connected and the communication link of the receipt card 31 and the liquidation terminal 12 is attained, the liquidation demand containing the frame (usually total amount) of the value which the receipt card 31 liquidates will be transmitted to the liquidation terminal 12 (step 521). Although the receipt card 31 compounds the random number R1 and the status S1 which were generated with the mutual recognition means 311 of the receipt card 31 to the enciphered liquidation demand and is transmitted to it at this time Like the mutual recognition explained on the occasion of above-mentioned value restoration, this is used, in order that said mutual recognition means 311 and mutual recognition means 121 of the liquidation terminal 12 may perform mutual recognition, and hereafter, although mutual recognition is performed for every communication link, since the authentication approach is the same, explanation is omitted here.

[0068] Next, the notice demand of ID is transmitted so that the liquidation terminal 12 which received the liquidation demand may notify the owner ID whom the receipt card 31 has to the receipt card 31 (step 522), and the owner ID of a proper is transmitted to the owner (vender 3) of the receipt card 31 with which the receipt card 31 which received this is stored in the owner ID storing

means 315 of the receipt card 31 at the liquidation terminal 12 (step 523).

[0069] The liquidation terminal 12 which received Owner ID transmits the subtraction demand according to an adjusted amount to the receipt card 31 (step 524).

[0070] With the receipt card 31 which received the subtraction demand, while subtracting the value that the value addition-and-subtraction means 312 of the receipt card 31 is stored in the value storing means 313 according to the subtraction demand, an addition demand is transmitted to the liquidation terminal 12 (step 525). The card ID (it is ID of a proper to the debit card which became an issue place at the time of value issue) memorized corresponding to the value (the value addition-and-subtraction means 312 subtracted) stored in the value storing means 313 is contained in this addition demand.

[0071] While storing the value according to an addition demand to the value storing means 122 of the liquidation terminal 12 (addition), based on the frame of the value corresponding to Card ID and this by which the outstanding-balance-of-issue-amount management tool 124 of the liquidation terminal 12 is contained in an addition demand, the contents of storage of the outstanding-balance-of-issue-amount management database 13 update, liquidation termination notifies to the receipt card 31, and liquidation processing ends with the liquidation terminal 12 which received the addition demand (step

526).

[0072] In the above, although migration of the value in the case of restoration of value, dealings, and liquidation was explained, the flow of value and detection of a malfeasance are explained here.

[0073] The debit card 21 which a user 2 owns from the restoration terminal 11 is filled up with the value which the card publisher 1 publishes. At this time, the restoration terminal 11 makes a pair the filled frame of value and the filled card ID of the debit card 21 of a restoration place, and records them on the outstanding-balance-of-issue-amount management database 13. Moreover, in case the debit card 21 filled up once is further filled up with value, with reference to the outstanding-balance-of-issue-amount management database 13, it is filled up within the limits of the issue limit of the value over a debit card 21 (only when the issue limit is set up), and after restoration breaks record of the outstanding-balance-of-issue-amount management database 13.

[0074] If a user 2 receives offer of goods or service from a vender 3, value will be moved to the receipt card 31 through the dealings terminal 32 as the countervalue from a debit card 21.

[0075] In case a vender 3 liquidates and encashes the value received from the user 2, he moves the value stored in the receipt card 31 to the card publisher's 1 liquidation terminal 12. At this time, the liquidation terminal 12 breaks record of

the outstanding-balance-of-issue-amount management database 13 based on the card ID number corresponding to the value frame of value and this which were moved from the receipt card 31.

[0076] In each process of restoration of value, dealings, and liquidation, since value by the side of a receptacle is increased and value is moved after the cut of the value by the side of delivery, performing mutual recognition by the delivery [of value], and receptacle side as mentioned above, even if it is difficult to forge a debit card 21 and the receipt card 31 and operates drawing out a card during migration of value etc., value cannot be increased.

[0077] Moreover, even if forgery of a card, reproduction of value, etc. are performed, the card publisher 1 can detect a malfeasance based on record of the outstanding-balance-of-issue-amount management database 13.

[0078] Drawing 8 is a flow chart which shows the flow of detection of a malfeasance. The outstanding-balance-of-issue-amount management database 13 starts actuation (step 601), when there is an update process to the frame of the value by restoration or liquidation, the record about the value of performing YES) and its update process, and the corresponding card ID is searched with the (step 602 (step 603), and the record (restoration or liquidation value frame) is broken (step 604).

[0079] As a result of renewal of record, when the direction of the value frame

liquidated rather than the filled value frame becomes large, it detects that YES) and a malfeasance were performed at the (step 605 (step 606), and unjust detection processing is ended (step 607).

[0080] When injustice is detected, it pursues based on the owner ID of the receipt card 31 acquired at the time of liquidation, value, and the corresponding card ID.

[0081] Moreover, the card can be made into an unjust proof, when it constituted so that the contents might be recorded as hysteresis whenever it moved value to both debit card 21 and receipt card 31 and injustice arises.

[0082] In addition, since it is not necessary to register the relation between Card ID and a user 2 also when predetermined effectiveness is acquired by the security top also when it is used without giving Card ID to a debit card 21, and Card ID is attached, it is possible to maintain a user's 2 privacy.

[0083] Next, the 2nd example of the settlement-of-accounts approach and system using the IC card concerning this invention is explained.

[0084] In this 2nd example, management and unjust detection of the value which attached and published the issue number (identification number) in the value which a card publisher publishes, and was published by using this issue number are performed.

[0085] The system in this 2nd example consists of the restoration terminal 11

and the liquidation terminal 12 which the card publisher 1 has, the outstanding-balance-of-issue-amount management database 13, the debit card 21 which a user 2 has and the receipt card 31 which a vender 3 has, and a dealings terminal 32 like the 1st above-mentioned example (refer to drawing 1).

[0086] Moreover, only a point which is different since each part which constitutes a system is the same as that of the 1st above-mentioned example almost is explained.

[0087] In the 2nd example, in order to perform management and unjust detection of the value published using the issue number given to value, a debit card 21 does not need to store the card ID of a proper in this card, and does not possess the card ID storing means 215 of a debit card 21. Moreover, the value restoration means 112 of the restoration terminal 11, the outstanding-balance-of-issue-amount management tool 114 and the value storing means 122 of the liquidation terminal 12, the outstanding-balance-of-issue-amount management tool 124, the value storing means 212 of a debit card 21, and the value storing means 312 of the receipt card 31 process by making the issue number always given to value and its value correspond.

[0088] That is, an issue number is surely given to the value published from the restoration terminal 11, and although the value published to the same debit card

21 to time amount with this same issue number serves as the same number, it becomes a different issue number at the value published to different time amount or a different debit card 21. In case a debit card 21 moves value to the receipt card 31 by dealings, it is moved by making the issue number of value and its value into a pair. Since value is divided when the frame of value which moves by dealings is smaller than the frame which received issue from the restoration terminal 11 at this time, value with the same issue number will exist.

[0089] Therefore, the outstanding-balance-of-issue-amount management database 13 accumulates the liquidated value for every issue number, and when the value that the adjusted amount exceeded the amount of issue is detected, it considers it as unjust detection.

[0090] In addition, also in this 2nd example, a delivery [of value] and receptacle side attests mutually like the 1st example in the case of migration of value.

[0091] Next, the 3rd example of the settlement-of-accounts approach and system using the IC card concerning this invention is explained.

[0092] This 3rd example uses the card provided in the IC card of one sheet by using both debit card 21 in the 1st above-mentioned example and 2nd above-mentioned example, and receipt card 31 as an income-and-outgo card.

[0093] Drawing 9 is the block diagram showing the configuration of an income-and-outgo card. The income-and-outgo card 41 possesses the mutual

recognition means 411, the value addition-and-subtraction means 412, the value storing means 413, the ** / receiving means 414, the owner ID storing means 415, and the card ID storing means 416, and is constituted. The mutual-recognition means 411 is a means attest mutually the restoration terminal 11 connected through ** / receiving means 414, the liquidation terminal 12, a debit card 21, the receipt card 31, other income-and-outgo card 41, and its justification, and the value addition-and-subtraction means 412 performs the addition and subtraction of value which are stored in the value storing means 413 for migration of worth of the partner attested by the mutual recognition means 411.

[0094] This income-and-outgo card 41 can be used as both debit card 21 in each above-mentioned example, and receipt card 31, and since that actuation is the same as that of an above-mentioned example, explanation is omitted.

[0095] In addition, when making it correspond to the 2nd above-mentioned example, it is not necessary to provide the card ID storing means 416 which the income-and-outgo card 41 possesses.

[0096] Moreover, as each above-mentioned example explained, in case value is moved to the receipt card 31 (or income-and-outgo card 41) from a debit card 21 (or income-and-outgo card 41), the dealings terminal 32 does not intervene in both communication link. That is, the dealings terminal 32 is not participating in

the security of the settlement system in each example.

[0097] Therefore, migration of value on the receipt card 31 (or income-and-outgo card 41) from a debit card 21 (or income-and-outgo card 41) can also be performed through a communication line. This communication line can also use the low thing of security nature like things which have comparatively high security nature, such as a dedicated line and the telephone line, or the Internet.

[0098] For example, as shown in drawing 10 (a), value can be moved between the terminal 51-1 connected to the Internet 50 thru/or either of 51-6, and it can also use for settlement of the on-line shopping on the Internet. Also at the terminal of dedication, each terminal 51-1 in this case thru/or 51-6 may connect IC card reader writer to a personal computer etc., and may use this as a terminal.

[0099] Moreover, as shown in drawing 10 (b), two or more terminals 61-1 which insert a debit card 21 (or income-and-outgo card 41) thru/or 61-4 can be connected to the terminal 60 which inserts the receipt card 31 (or income-and-outgo card 41), and value can be moved to it. At a store etc., the system shown in this drawing 10 (b) can be used, when collecting all the sales on one receipt card by installing a terminal 60 in an office and arranging a terminal 61-1 thru/or 61-4 to a register, respectively.

[0100] In addition, in each above-mentioned example, the use range can also be further extended by preparing a cash **** function, an account draw-down

function, a credit settlement-of-accounts function, etc. in the restoration terminal 11, and preparing a cash expenditure function, an account transfer function, etc. in the liquidation terminal 12.

[0101]

[Effect of the Invention] As explained above, according to this invention, restoration of worth of a debit card and dealings with a vender are conducted, without a user revealing a status. Since it constituted so that might reveal a status, value might be liquidated, a debit card and a receipt card might perform mutual recognition and a vender might move value While being able to protect a user's privacy, transfer of a debit card is attained, and since the dealings terminal at the time of moving value does not participate in the insurance of a system, it can mind a communication link or can install it broadly. Moreover, it can also make it difficult to perform injustice, such as tax evasion of a vender, in addition to injustice, such as use of forged value.

[0102] Moreover, a trace when injustice arises can be easily performed to a debit card by using the issue number of a proper etc. for ID and issue worth of a proper.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the system configuration of the settlement system using an IC card.

[Drawing 2] The block diagram showing the detail of a restoration terminal.

[Drawing 3] The block diagram showing the detail of a liquidation terminal.

[Drawing 4] The block diagram showing the detail of a debit card.

[Drawing 5] The block diagram showing the detail of a receipt card.

[Drawing 6] The block diagram showing the detail of a dealings terminal.

[Drawing 7] Drawing having shown each communication link data flow in the case of restoration of value, dealings, and liquidation.

[Drawing 8] The flow chart which shows the flow of detection of a malfeasance.

[Drawing 9] The block diagram showing the configuration of an income-and-outgo card.

[Drawing 10] Drawing having shown the example of use of a settlement system.

[Drawing 11] Drawing having shown the gestalt of the value stored in the IC card in the circulation process in the conventional system.

[Description of Notations]

1 Card Publisher

2 User

3 Vender

11 Restoration Terminal

12 Liquidation Terminal

13 Outstanding-Balance-of-Issue-Amount Management Database

21 Debit Card

31 Receipt Card

32 Dealings Terminal

41 Income-and-Outgo Card

50 Internet

51-1 to 51-6 Terminal

60 Terminal

61-1 to 61-4 Terminal

111 Mutual Recognition Means

112 Value Restoration Means

113 ** / Receiving Means

114 Outstanding-Balance-of-Issue-Amount Management Tool

121 Mutual Recognition Means

122 Value Storing Means

123 ** / Receiving Means

124 Outstanding-Balance-of-Issue-Amount Management Tool

211 Mutual Recognition Means

212 Value Addition-and-Subtraction Means

213 Value Storing Means

214 ** / Receiving Means

215 Card ID Storing Means

311 Mutual Recognition Means

312 Value Addition-and-Subtraction Means

313 Value Storing Means

314 ** / Receiving Means

315 Owner ID Storing Means

321 ** / Receiving Means

322 ** / Receiving Means

323 Notice Means of Dealings Initiation

411 Mutual Recognition Means

412 Value Addition-and-Subtraction Means

413 Value Storing Means

414 ** / Receiving Means

415 Owner ID Storing Means

416 Card ID Storing Means

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－203371

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	19/00		Ｇ０６Ｆ	15/30	３６０
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｔ
	19/10		Ｇ０７Ｄ	9/00	４３６Ｚ
Ｇ０７Ｄ	9/00	４３６	Ｇ０７Ｇ	1/12	３２１Ｐ
Ｇ０７Ｆ	7/08			1/14	

審査請求　未請求　請求項の数13　ＯＬ　（全 15 頁）　最終頁に続く

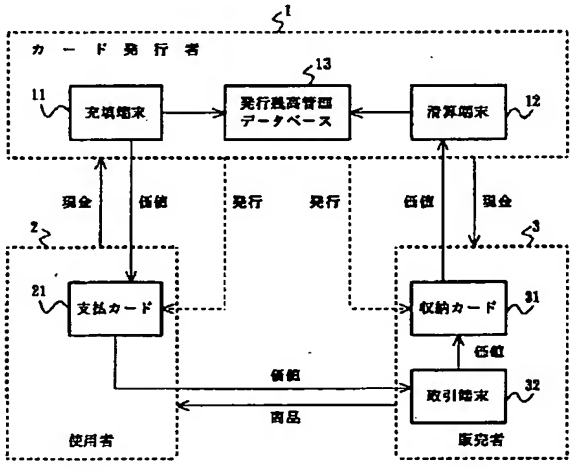
(21)出願番号　特願平10－2441

(22)出願日　平成10年(1998)１月８日

(71)出願人　000152859
株式会社日本コンラックス
東京都千代田区内幸町２丁目２番２号
(72)発明者　太田　通博
埼玉県坂戸市伊豆の山町55－２
(74)代理人　弁理士　木村　高久

(54)【発明の名称】　ＩＣカードを用いた決済方法およびシステム

(57)【要約】
【課題】匿名性を維持しつつ、不正があった場合の発見を早くし、かつ追跡が可能で利便性が高く比較的簡易な構成で実現できるＩＣカードを用いた決済方法およびシステムを提供する。
【解決手段】使用者（２）が身分を明かすことなく充填端末（１１）から支払カード（２１）への価値の充填を行い、販売者（３）との取引を行う際には、取引端末（３２）を単なる伝送手段として支払カード（２１）と収納カード（３１）が相互認証を行って価値を移動させる。



1

【特許請求の範囲】

【請求項１】　商品若しくはサービスの対価となる価値情報を格納したＩＣカードを利用し、前記価値情報を移動させることにより決済を行うＩＣカードを用いた決済方法において、

前記対価の支払者が使用する第１のＩＣカードと該第１のＩＣカードに前記価値情報を充填する充填端末とが相互認証を行い、該相互認証が成功した場合に前記充填端末から前記第１のＩＣカードに前記価値情報の充填を行い、

前記対価の支払者と該対価の受領者とが決済を行う際に、前記第１のＩＣカードと前記受領者が使用する第２のＩＣカードとが相互認証を行い、該相互認証が成功した場合に前記第１のＩＣカードから前記第２のＩＣカードへ前記価値情報の移動を行い、

前記第２のＩＣカードと該第２のＩＣカードから前記価値情報を受領して清算を行う清算端末とが相互認証を行い、該相互認証が成功した場合に前記第２のＩＣカードから前記清算端末に前記価値情報を移動して清算を行うことを特徴とするＩＣカードを用いた決済方法。

【請求項２】　前記第２のＩＣカードは、

前記受領者に固有の所有者識別符号を記憶し、前記清算端末へ前記価値情報を移動させる場合に、該価値情報の移動とともに前記所有者識別符号を通知することを特徴とする請求項１記載のＩＣカードを用いた決済方法。

【請求項３】　前記第１のＩＣカードは、

該第１のＩＣカードに固有のカード識別符号を記憶し、

前記充填端末は、前記価値情報の充填を行う場合に該価値情報の額と前記カード識別符号を対応させて発行残高管理データベースに記憶し、

前記第２のＩＣカードは、前記第１のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領し、

前記清算端末は、前記第２のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領するとともに、該受領した価値情報の額と該カード識別符号とを前記発行残高管理データベースに記憶し、

前記発行残高管理データベースは、前記カード識別符号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする請求項１または２記載のＩＣカードを用いた決済方法。

【請求項４】　前記充填端末は、

前記価値情報の充填を行う場合に該価値情報に固有の発行番号を付し、該価値情報の額と前記発行番号を対応させて発行残高管理データベースに記憶し、

前記第２のＩＣカードは、前記第１のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領し、

2

前記清算端末は、前記第２のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領するとともに、該受領した価値情報の額と該発行番号とを前記発行残高管理データベースに記憶し、

前記発行残高管理データベースは、前記発行番号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする請求項１または２記載のＩＣカードを用いた決済方法。

【請求項５】　前記相互認証は、

前記第１のＩＣカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第２のＩＣカードへ送信し、

前記暗号化送信情報が前記第２のＩＣカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較確認することで、前記第２のＩＣカードを認証し、

前記第２のＩＣカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第１のＩＣカードへ送信し、

前記暗号化送信情報が前記第１のＩＣカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較確認することで、前記第１のＩＣカードを認証することで行うことを特徴とする請求項１乃至４のいずれかに記載のＩＣカードを用いた決済方法。

【請求項６】　前記第１のＩＣカードと前記第２のＩＣカードとが、

同一のＩＣカード内に構成されることを特徴とする請求項１乃至５のいずれかに記載のＩＣカードを用いた決済方法。

【請求項７】　商品若しくはサービスの対価となる価値情報を格納したＩＣカードを利用し、前記価値情報を移動させることにより決済を行うＩＣカードを用いた決済システムにおいて、

前記対価の支払者が使用する第１のＩＣカードと、

前記対価の受領者が使用する第２のＩＣカードと、

前記第１のＩＣカードに前記価値情報を充填する充填端末と、

前記第２のＩＣカードから前記価値情報を受領して清算を行う清算端末と、

前記第１のＩＣカードと前記第２のＩＣカードとの間の通信を仲介する取引端末と、

前記充填端末が充填した価値情報の額と前記清算端末が清算した価値情報の額とを記憶管理する発行残高管理データベースとを具備し、

前記第１のＩＣカードは、前記充填端末と前記第２のＩ

Ｃカードとのいずれかとの間で相互認証を行う第１の相互認証手段と、前記価値情報を格納する第１の価値情報格納手段と、該第１の価値情報格納手段に格納された前記価値情報を移動させる第１の価値情報移動手段とを具備し、
前記第２のＩＣカードは、前記清算端末と前記第１のＩＣカードとのいずれかとの間で相互認証を行う第２の相互認証手段と、前記価値情報を格納する第２の価値情報格納手段と、該第２の価値情報格納手段に格納された前記価値情報を移動させる第２の価値情報移動手段とを具備し、
前記充填端末は、前記第１のＩＣカードとの間で相互認証を行う第３の相互認証手段と、前記価値情報を充填する価値情報充填手段と、該価値情報充填手段が充填した価値情報の額を前記発行残高管理データベースに記憶させる充填額記憶手段とを具備し、
前記清算端末は、前記第２のＩＣカードとの間で相互認証を行う第４の相互認証手段と、前記価値情報を受領して清算する価値情報清算手段と、該価値情報清算手段により清算された価値情報の額を前記発行残高管理データベースに記憶させる清算額記憶手段とを具備し、
前記取引端末は、前記第１のＩＣカードに決済取引の開始を通知する取引開始通知手段と、前記第１のＩＣカードと前記第２のＩＣカードとの間の通信を仲介する伝送手段とを具備することを特徴とするＩＣカードを用いた決済システム。
【請求項８】　前記第２のＩＣカードは、
前記受領者に固有の所有者識別符号を記憶する所有者識別符号格納手段と、
前記清算端末との間で清算を行う場合に、前記第２の価値情報移動手段による価値情報の移動とともに前記所有者識別符号を前記清算端末に通知する所有者識別符号通知手段とをさらに具備することを特徴とする請求項７記載のＩＣカードを用いた決済システム。
【請求項９】　前記第１の価値情報移動手段は、
前記第１の価値情報格納手段に格納される価値情報の加減算を行う第１の価値情報加減算手段を具備し、前記充填端末から価値情報の充填を受けるときは前記第１の価値情報加減算手段が前記第１の価値情報格納手段に格納されている価値情報に充填額を加算し、前記第２のＩＣカードへの価値情報の支払を行う場合には前記第１の価値情報加減算手段が前記第１の価値情報格納手段に格納されている価値情報から支払額を減算し、
前記第２の価値情報移動手段は、
前記第２の価値情報格納手段に格納される価値情報の加減算を行う第２の価値情報加減算手段を具備し、前記第１のＩＣカードから価値情報を受領するときは前記第２の価値情報加減算手段が前記第２の価値情報格納手段に格納されている価値情報に受領額を加算し、前記清算端末との間で清算を行う場合には前記第２の価値情報加減算手段が前記第２の価値情報格納手段に格納されている価値情報から清算額を減算することを特徴とする請求項７記載のＩＣカードを用いた決済システム。
【請求項１０】　前記第１のＩＣカードは、
該第１のＩＣカードに固有のカード識別符号を格納するカード識別符号格納手段と、前記充填端末から価値情報の充填を受ける場合に前記カード識別符号を該充填端末に通知するカード識別符号通知手段とをさらに具備し、
前記充填額記憶手段は、前記価値情報充填手段が前記第１のＩＣカードに充填する価値情報の額と前記カード識別符号通知手段により通知されたカード識別符号とを対応させて前記発行残高管理データベースへ記憶し、
前記第１の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、
前記第２の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、
前記第２の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記カード識別符号とを対応させて格納し、
前記清算額記憶手段は、前記清算額記憶手段が前記第２のＩＣカードとの間で清算する価値情報の額と前記カード識別符号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする請求項７または８記載のＩＣカードを用いた決済システム。
【請求項１１】　前記価値情報充填手段は、
前記価値情報の充填を行う場合に該価値情報に固有の発行番号を生成する発行番号生成手段をさらに具備し、
前記充填額記憶手段は、前記価値情報充填手段が前記第１のＩＣカードに充填する価値情報の額と前記発行番号生成手段により生成された発行番号とを対応させて前記発行残高管理データベースへ記憶し、
前記第１の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、
前記第１の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、
前記第２の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、
前記第２の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、
前記清算額記憶手段は、前記清算額記憶手段が前記第２のＩＣカードとの間で清算する価値情報の額と前記発行番号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする請求項７または８記載のＩＣカードを用いた決済システム。

【請求項１２】　前記第１の相互認証手段と前記第２の相互認証手段と前記第３の相互認証手段と前記第４の相互認証手段とは、
任意の乱数を発生させる乱数発生手段と、該乱数発生手段が発生した乱数と所定の情報とを合成する合成手段と、該合成手段の出力を暗号化する暗号化手段と、暗号化された受信情報を復号化する復号化手段と、該復号化手段により復号化された情報を所定の情報と乱数とに分離する分離手段をさらに具備し、
前記乱数発生手段が発生した乱数を前記合成手段で所定の情報と合成して前記暗号化手段で暗号化して送信するとともに、
該送信先で復号化および分離された前記乱数が前記所定の情報に対する返信情報に合成されて暗号化されたことを、該暗号化された返信情報を前記復号化手段で復号化して前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とを前記比較手段で比較し、
該比較の結果、前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とが同一であった場合に前記送信先が同一の暗号鍵を有する正当な通信相手であると認証することを特徴とする請求項７乃至１１のいずれかに記載のＩＣカードを用いた決済システム。
【請求項１３】　前記第１のＩＣカードと前記第２のＩＣカードとが、
同一のＩＣカード内に構成されることを特徴とする請求項７乃至１２のいずれかに記載のＩＣカードを用いた決済システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、ＩＣカードを用いた決済方法およびシステムに関し、特に、比較的簡易な構成で、匿名性を維持し、不正の早期検出や価値の転々流通を行うことのできるＩＣカードを用いた決済方法およびシステムに関する。
【０００２】
【従来技術】ＩＣカードを用いて決済を行う決済システムは、価値ベースの決済と信用ベースの決済とに分類できる。価値ベースの決済は、比較的に現金による決済に近く、ＩＣカードに価値が充填されていて、その価値を移動することで決済するものである。信用ベースの決済は、クレジットカードを利用した決済システムに代表されるように、ＩＣカードに記録された個人情報に基づいて承認行為を行い、オンライン口座資金移動によって決済するものである。
【０００３】また、価値ベースの決済は、その価値の移動形態から現金型と前払型に分類することができる。
【０００４】現金型では、現金での取引と同様に、取引により受け取った価値を別の取引の支払に利用することができる。このため、現金型には匿名性、つまり誰が何処でどの様な取引を行ったかは追跡されないが、価値が転々流通するために偽造価値が混入された場合、それを発見することは困難である。

【０００５】前払型では、価値の発行元がＩＣカードに充填した価値は、一度取引された後に、必ず価値の発行元で清算する、つまり商品を購入した場合にはその価値は商品と引き替えに消滅（清算以外の使用不能）することになる。また、使用時に暗証番号を必要とすることが多い。このため、偽造価値の混入等の不正に対しては強固なシステムであるが、匿名性が無く、利便性にも欠けることになる。
【０００６】このように、現金型と前払型には夫々長所と短所があるが、最近では現金型と前払型の長所を兼ね備えた決済システムも提案されている。
【０００７】この決済システムは、匿名性を維持しつつも不正が行われた場合には、一定の追跡ができるシステムであり、例えば、ＩＣカードの利用者の他に、登録機関と発行機関、金融機関で構成されるシステムである。
【０００８】登録機関は、利用者が利用する公開鍵（秘密鍵と対をなして使用する暗号鍵であり、秘密鍵は利用者のみが知り得る暗号鍵）と利用者の名前を対にして登録しておき、この公開鍵の正当性を第三者に対して保証する。また、この公開鍵は登録機関のディジタル署名と併せて登録書としてＩＣカードに格納される。
【０００９】発行機関は、価値の発行と管理、不正の検出を行うが、利用者は発行機関に対して名前を明かさず、登録機関の保証の元に公開鍵を名前の代わり、つまり仮名として利用することでＩＣカードへの価値の充填を行うことができるため匿名性を維持できる。
【００１０】金融機関は利用者の口座を管理し、発行機関でのＩＣカードへの価値の充填に必要な依頼書を利用者の要請に基づき発行するが、利用者の仮名（公開鍵）と実名が一致しないようにブラインド署名という技術を用いて、利用者の仮名が金融機関に知られることなく、依頼書を発行することができる。
【００１１】ここで、発行機関が発行した価値の流通について説明する。図１１は、流通過程でのＩＣカード内に格納されている価値の形態を示した図である。
【００１２】図１１（ａ）は、発行機関が利用者Ａ（仮名ａａａ）に対して発行した価値を示しており、価値１０１１には、その価値の額面１０１２（１００００円）と識別番号１０１３（ｘｘｘｘｘ：紙幣に付された紙幣番号のようなもの）、発行先の仮名１０１４（ａａａ）、発行機関のディジタル署名１０１５が付されている。
【００１３】利用者Ａがこの価値１０１１の全部または一部を利用者Ｂ（仮名ｂｂｂ）へ対価として支払または譲渡する場合には、図１１（ｂ）に示すように価値１０１１に譲渡証を添付して支払または譲渡する。
【００１４】図１１（ｂ）に示す譲渡証１０２１は、価値１０１１の他に譲渡する額面１０２２（４５００円）

と譲渡証番号１０２３（ｙｙｙｙｙ）、譲渡先の仮名１０２４（ｂｂｂ）、利用者Ａの署名１０２５（ａａａ）が付されている。署名１０２５は、利用者Ａのみが知っている（はず）の秘密鍵で価値１０１１と額面１０２２、譲渡証番号１０２３、仮名１０２４を暗号化することで行われており、利用者Ｂは公開されている公開鍵（仮名として利用されているａａａ）で復号化することで検証できる。また、譲渡証番号１０２３は、同じ番号が生じないように受け取り側（利用者Ｂ）の責任で決定する。

【００１５】利用者Ａは、他の利用者への価値１０１１の譲渡等を行うこともできるが、譲渡した価値の額面の総和が額面１０１２（１００００円）を越えることができないのはいうまでもない（利用者Ａの所有するＩＣカードの制御による）。

【００１６】同様に、利用者Ｂが利用者Ｃ（仮名ｃｃｃ）へ価値の譲渡等を行う場合には、図１１（ｃ）に示すように価値１０１１を含む譲渡証１０２１にさらに譲渡証１０３１を添付して譲渡等を行う。図１１（ｃ）に示す譲渡証１０３１は、譲渡証１０２１の他に譲渡する額面１０３２（２１００円）と譲渡証番号１０３３（ｚｚｚｚｚ）、譲渡先の仮名１０３４（ｃｃｃ）、利用者Ｂの署名１０３５（ｂｂｂ）が付されている。この署名１０３５も同様に利用者Ｂのみが知っている秘密鍵を利用して行われる。

【００１７】このように価値１０１１は、任意の額面で分割して譲渡することができ、譲渡証の連鎖により転々と流通する。

【００１８】ところで、この価値１０１１の流通の過程で不正が生じたとしても、最終的に発行機関での清算（価値の回収）の際に発見することができる。例えば、利用者Ｂが利用者Ａから譲渡を受けた価値１０１１（譲渡証１０２１）をコピーして何度も利用したとする。この場合、利用者Ｂが利用できるのは譲渡先が自分に指定された譲渡証１０２１のみであり（価値１０１１を抽出してコピーしようとしても、発行先の指定がａａａであるので譲渡される側が受け取りを拒否する）、譲渡証１０２１は署名１０２５で暗号化されているため譲渡証番号１０２３を書き換えることができない。したがって、譲渡証１０２１をコピーしても同一の譲渡証番号が付されたままとなり、これらを使用すれば、発行機関で譲渡証番号に基づいて不正をおこなった人物が利用者Ｂであると特定される。発行機関は、利用者Ｂが不正を行ったことを特定できれば登録機関に問い合わせ、利用者Ｂの実名を取得して摘発することができる。

【００１９】

【発明が解決しようとする課題】ところが、上述の現金型と前払型の長所を兼ね備えた決済システムでは、不正が行われた際に、この不正が発見されるまでに要する時間が長く、盗難カードに基づいて不正が行われた場合には、追跡がほぼ不可能となる。

【００２０】また、利用者が使用する各ＩＣカードでは多量のメモリと計算時間を必要とするためコストが高くなるといった問題点があった。

【００２１】そこで、この発明は、匿名性を維持しつつ、不正があった場合の発見を早くし、かつ追跡が可能で利便性が高く比較的簡易な構成で実現できるＩＣカードを用いた決済方法およびシステムを提供することを目的とする。

【００２２】

【課題を解決するための手段】上述した目的を達成するため、請求項１の発明では、商品若しくはサービスの対価となる価値情報を格納したＩＣカードを利用し、前記価値情報を移動させることにより決済を行うＩＣカードを用いた決済方法において、前記対価の支払者が使用する第１のＩＣカードと該第１のＩＣカードに前記価値情報を充填する充填端末とが相互認証を行い、該相互認証が成功した場合に前記充填端末から前記第１のＩＣカードに前記価値情報の充填を行い、前記対価の支払者と該対価の受領者とが決済を行う際に、前記第１のＩＣカードと前記受領者が使用する第２のＩＣカードとが相互認証を行い、該相互認証が成功した場合に前記第１のＩＣカードから前記第２のＩＣカードへ前記価値情報の移動を行い、前記第２のＩＣカードと該第２のＩＣカードから前記価値情報を受領して清算を行う清算端末とが相互認証を行い、該相互認証が成功した場合に前記第２のＩＣカードから前記清算端末に前記価値情報を移動して清算を行うことを特徴とする。

【００２３】また、請求項２の発明では、請求項１の発明において、前記第２のＩＣカードは、前記受領者に固有の所有者識別符号を記憶し、前記清算端末へ前記価値情報を移動させる場合に、該価値情報の移動とともに前記所有者識別符号を通知することを特徴とする。

【００２４】また、請求項３の発明では、請求項１または２の発明において、前記第１のＩＣカードは、該第１のＩＣカードに固有のカード識別符号を記憶し、前記充填端末は、前記価値情報の充填を行う場合に該価値情報の額と前記カード識別符号を対応させて発行残高管理データベースに記憶し、前記第２のＩＣカードは、前記第１のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領し、前記清算端末は、前記第２のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記カード識別符号と対応させて受領するとともに、該受領した価値情報の額と該カード識別符号とを前記発行残高管理データベースに記憶し、前記発行残高管理データベースは、前記カード識別符号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする。

【００２５】また、請求項４の発明では、請求項１また

は２の発明において、前記充填端末は、前記価値情報の充填を行う場合に該価値情報に固有の発行番号を付し、該価値情報の額と前記発行番号を対応させて発行残高管理データベースに記憶し、前記第２のＩＣカードは、前記第１のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領し、前記清算端末は、前記第２のＩＣカードから前記価値情報を受領する場合に、該価値情報を前記発行番号と対応させて受領するとともに、該受領した価値情報の額と該発行番号とを前記発行残高管理データベースに記憶し、前記発行残高管理データベースは、前記発行番号に対応した前記価値の総充填額と総受領額とを比較し、該比較結果に基づいて不正行為を検出することを特徴とする。

【００２６】また、請求項５の発明では、請求項１乃至４のいずれかの発明において、前記相互認証は、前記第１のＩＣカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第２のＩＣカードへ送信し、前記暗号化送信情報が前記第２のＩＣカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較することで確認することで、前記第２のＩＣカードを認証し、前記第２のＩＣカードが、任意の乱数を発生し、該発生した乱数を所定の送信情報に合成して暗号化した暗号化送信情報を前記第１のＩＣカードへ送信し、前記暗号化送信情報が前記第１のＩＣカードで復号化されて前記乱数と分離され、該分離された乱数が所定の返信情報に合成されて暗号化された暗号化返信情報として返信されたことを、前記暗号化返信情報を復号化して分離した乱数と前記発生した乱数とを比較確認することで、前記第１のＩＣカードを認証することで行うことを特徴とする。

【００２７】また、請求項６の発明では、請求項１乃至５のいずれかの発明において、前記第１のＩＣカードと前記第２のＩＣカードとが、同一のＩＣカード内に構成されることを特徴とする。

【００２８】また、請求項７の発明では、商品若しくはサービスの対価となる価値情報を格納したＩＣカードを利用し、前記価値情報を移動させることにより決済を行うＩＣカードを用いた決済システムにおいて、前記対価の支払者が使用する第１のＩＣカードと、前記対価の受領者が使用する第２のＩＣカードと、前記第１のＩＣカードに前記価値情報を充填する充填端末と、前記第２のＩＣカードから前記価値情報を受領して清算を行う清算端末と、前記第１のＩＣカードと前記第２のＩＣカードとの間の通信を仲介する取引端末と、前記充填端末が充填した価値情報の額と前記清算端末が清算した価値情報の額とを記憶管理する発行残高管理データベースとを具備し、前記第１のＩＣカードは、前記充填端末と前記第２のＩＣカードとのいずれかとの間で相互認証を行う第１の相互認証手段と、前記価値情報を格納する第１の価値情報格納手段と、該第１の価値情報格納手段に格納された前記価値情報を移動させる第１の価値情報移動手段とを具備し、前記第２のＩＣカードは、前記清算端末と前記第１のＩＣカードとのいずれかとの間で相互認証を行う第２の相互認証手段と、前記価値情報を格納する第２の価値情報格納手段と、該第２の価値情報格納手段に格納された前記価値情報を移動させる第２の価値情報移動手段とを具備し、前記充填端末は、前記第１のＩＣカードとの間で相互認証を行う第３の相互認証手段と、前記価値情報を充填する価値情報充填手段と、該価値情報充填手段が充填した価値情報の額を前記発行残高管理データベースに記憶させる充填額記憶手段とを具備し、前記清算端末は、前記第２のＩＣカードとの間で相互認証を行う第４の相互認証手段と、前記価値情報を受領して清算する価値情報清算手段と、該価値情報清算手段により清算された価値情報の額を前記発行残高管理データベースに記憶させる清算額記憶手段とを具備し、前記取引端末は、前記第１のＩＣカードに決済取引の開始を通知する取引開始通知手段と、前記第１のＩＣカードと前記第２のＩＣカードとの間の通信を仲介する伝送手段とを具備することを特徴とする。

【００２９】また、請求項８の発明では、請求項７の発明において、前記第２のＩＣカードは、前記受領者に固有の所有者識別符号を記憶する所有者識別符号格納手段と、前記清算端末との間で清算を行う場合に、前記第２の価値情報移動手段による価値情報の移動とともに前記所有者識別符号を前記清算端末に通知する所有者識別符号通知手段とをさらに具備することを特徴とする。

【００３０】また、請求項９の発明では、請求項７の発明において、前記第１の価値情報移動手段は、前記第１の価値情報格納手段に格納される価値情報の加減算を行う第１の価値情報加減算手段を具備し、前記充填端末から価値情報の充填を受けるときは前記第１の価値情報加減算手段が前記第１の価値情報格納手段に格納されている価値情報に充填額を加算し、前記第２のＩＣカードへの価値情報の支払を行う場合には前記第１の価値情報加減算手段が前記第１の価値情報格納手段に格納されている価値情報から支払額を減算し、前記第２の価値情報移動手段は、前記第２の価値情報格納手段に格納される価値情報の加減算を行う第２の価値情報加減算手段を具備し、前記第１のＩＣカードから価値情報を受領するときは前記第２の価値情報加減算手段が前記第２の価値情報格納手段に格納されている価値情報に受領額を加算し、前記清算端末との間で清算を行う場合には前記第２の価値情報加減算手段が前記第２の価値情報格納手段に格納されている価値情報から清算額を減算することを特徴とする。

【００３１】また、請求項１０の発明では、請求項７ま

たは８の発明において、前記第１のＩＣカードは、該第１のＩＣカードに固有のカード識別符号を格納するカード識別符号格納手段と、前記充填端末から価値情報の充填を受ける場合に前記カード識別符号を該充填端末に通知するカード識別符号通知手段とをさらに具備し、前記充填額記憶手段は、前記価値情報充填手段が前記第１のＩＣカードに充填する価値情報の額と前記カード識別符号通知手段により通知されたカード識別符号とを対応させて前記発行残高管理データベースへ記憶し、前記第１の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、前記第２の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記カード識別符号とを対応させて移動し、前記第２の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記カード識別符号とを対応させて格納し、前記清算額記憶手段は、前記清算額記憶手段が前記第２のＩＣカードとの間で清算する価値情報の額と前記カード識別符号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする。

【００３２】また、請求項１１の発明では、請求項７または８の発明において、前記価値情報充填手段は、前記価値情報の充填を行う場合に該価値情報に固有の発行番号を生成する発行番号生成手段をさらに具備し、前記充填額記憶手段は、前記価値情報充填手段が前記第１のＩＣカードに充填する価値情報の額と前記発行番号生成手段により生成された発行番号とを対応させて前記発行残高管理データベースへ記憶し、前記第１の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、前記第１の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、前記第２の価値情報移動手段は、前記価値情報を移動させる場合に該価値情報と前記発行番号とを対応させて移動し、前記第２の価値情報格納手段は、前記価値情報を格納する場合に該価値情報と前記発行番号とを対応させて格納し、前記清算額記憶手段は、前記清算額記憶手段が前記第２のＩＣカードとの間で清算する価値情報の額と前記発行番号とを対応させて前記発行残高管理データベースへ記憶することを特徴とする。

【００３３】また、請求項１２の発明では、請求項７乃至１１のいずれかの発明において、前記第１の相互認証手段と前記第２の相互認証手段と前記第３の相互認証手段と前記第４の相互認証手段とは、任意の乱数を発生させる乱数発生手段と、該乱数発生手段が発生した乱数と所定の情報とを合成する合成手段と、該合成手段の出力を暗号化する暗号化手段と、暗号化された受信情報を復号化する復号化手段と、該復号化手段により復号化された情報を所定の情報と乱数とに分離する分離手段をさらに具備し、前記乱数発生手段が発生した乱数を前記合成手段で所定の情報と合成して前記暗号化手段で暗号化して送信するとともに、該送信先で復号化および分離された前記乱数が前記所定の情報に対する返信情報に合成されて暗号化されたことを、該暗号化された返信情報を前記復号化手段で復号化して前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とを前記比較手段で比較し、該比較の結果、前記分離手段で分離した乱数と前記乱数発生手段が発生した乱数とが同一であった場合に前記送信先が同一の暗号鍵を有する正当な通信相手であると認証することを特徴とする。

【００３４】また、請求項１３の発明では、請求項７乃至１２のいずれかの発明において、前記第１のＩＣカードと前記第２のＩＣカードとが、同一のＩＣカード内に構成されることを特徴とする。

【００３５】

【発明の実施の形態】以下、この発明に係わるＩＣカードを用いた決済方法およびシステムの一実施例を添付図面を参照して詳細に説明する。

【００３６】図１は、決済システムのシステム構成を示すブロック図である。決済システムは、カード発行者１が有する充填端末１１と清算端末１２と発行残高管理データベース１３、使用者２が有する支払カード２１、販売者３が有する収納カード３１と取引端末３２で構成される。

【００３７】充填端末１１は、支払カード２１に商品やサービス等の対価となる価値を充填し、清算端末１２は収納カード３１から価値を回収する。発行残高管理データベース１３は、発行済みで未回収の残高を記憶するデータベースである。

【００３８】使用者２が販売者３から商品やサービス等の提供を受け、その対価として価値を支払う際には、取引端末３２を介して支払カード２１から収納カード３１へ価値の移動を行う。

【００３９】図２は、充填端末１１の詳細を示すブロック図である。充填端末１１は、相互認証手段１１１、価値充填手段１１２、送／受信手段１１３、発行残高管理手段１１４を具備して構成される。相互認証手段１１１は、送／受信手段１１３を介して接続される支払カード２１とその正当性を相互に認証する手段であり、価値充填手段１１２は相互認証手段１１１により支払カード２１が認証された場合に支払カード２１に価値を充填する。発行残高管理手段１１４は、発行残高管理データベース１３に記憶されている価値の発行残高の参照や更新を行う。

【００４０】図３は、清算端末１２の詳細を示すブロック図である。清算端末１２は、相互認証手段１２１、価値格納手段１２２、送／受信手段１２３、発行残高管理手段１２４を具備して構成される。相互認証手段１２１は、送／受信手段１２３を介して接続される収納カード３１とその正当性を相互に認証する手段であり、価値格

納手段１２２は相互認証手段１２１により収納カード３１が認証された場合に収納カード３１から価値を受領して格納する。発行残高管理手段１２４は、発行残高管理データベース１３に記憶されている価値の発行残高の参照や更新を行う。

【００４１】図４は、支払カード２１の詳細を示すブロック図である。支払カード２１は、相互認証手段２１１、価値加減算手段２１２、価値格納手段２１３、送／受信手段２１４、カードＩＤ格納手段２１５を具備して構成される。相互認証手段２１１は、送／受信手段２１４を介して接続される充填端末１１や収納カード３１とその正当性を相互に認証する手段であり、価値加減算手段２１２は、相互認証手段２１１により充填端末１１が認証されれば充填端末１１から充填される価値を価値格納手段２１３に格納されている価値に加算し、収納カード３１が認証されれば、価値格納手段２１３に格納されている価値をその取引額に応じて減算する。また、カードＩＤ格納手段２１５は、支払カード２１に固有のカードＩＤ番号を格納する手段であり、このカードＩＤ番号により発行者１は発行済みの価値の管理を行う。

【００４２】図５は、収納カード３１の詳細を示すブロック図である。収納カード３１は、相互認証手段３１１、価値加減算手段３１２、価値格納手段３１３、送／受信手段３１４、所有者ＩＤ格納手段３１５を具備して構成される。相互認証手段３１１は、送／受信手段３１４を介して接続される清算端末１２や支払カード２１とその正当性を相互に認証する手段であり、価値加減算手段３１２は、相互認証手段３１１により清算端末１２が認証されればから価値格納手段３１３に格納されている価値を減算して清算端末１２へ渡し、支払カード２１が認証されれば、支払カード２１から取引額に応じた価値を受領して価値格納手段３１３に格納されている価値に加算する。また、所有者ＩＤ格納手段３１５は、収納カード３１の所有者に固有の所有者ＩＤ番号を格納する手段である。

【００４３】図６は、取引端末３２の詳細を示すブロック図である。取引端末３２は、支払カード２１と接続される送／受信手段３２１と収納カード３１と接続される送／受信手段３２２と支払カード２１に取引の開始を通知する取引介し通知手段３２３を具備して構成される。取引端末３２は、取引開始通知手段３２３が発生する取引開始要求を除いて送／受信手段３２１と送／受信手段３２２が送受するデータには介入しない。

【００４４】ここで、図７を参照して、価値の充填、取引、清算の際の充填端末１１、清算端末１２、支払カード２１、収納カード３１、取引端末３２の動作および通信データの流れを説明する。

【００４５】図７は、価値の充填、取引、清算の際の各々の通信データの流れを示した図である。

【００４６】図７（ａ）は、価値充填の際に支払カード２１と充填端末１１との間で授受されるデータの流れを示した図である。

【００４７】まず、支払カード２１が充填端末１１に挿入され、支払カード２１の送／受信手段２１４と充填端末１１の送／受信手段１１３が接続されて支払カード２１と充填端末１１が通信可能な状態になると、支払カード２１が充填要求を充填端末１１に送信する（ステップ５０１）。このとき、充填要求は支払カード２１の相互認証手段２１１で数０と合成されて暗号化され、さらに該相互認証手段２１１が発生した乱数Ｒ１とステータスＳ１が付加されて送信される。

【００４８】充填要求を受信した充填端末１１は、この充填端末１１の相互認証手段１１１で乱数Ｒ１とステータスＳ１を分離した後、復号化および数０との分離を行うことで充填要求を受信する。次に、充填端末１１は支払カード２１に該支払カードのカードＩＤを通知することを要求するが、このとき、前記相互認証手段１１１が先に分離した乱数Ｒ１とＩＤ通知要求を合成して暗号化し、この暗号化情報にさらに前記相互認証手段１１１が発生した乱数Ｒ２とステータスＳ２を合成した合成情報を支払カード２１に送信する（ステップ５０２）。

【００４９】合成情報を受信した支払カード２１は、この支払カード２１の相互認証手段２１１で受信した合成情報から乱数Ｒ２とステータスＳ２を分離して暗号化情報を取得し、この暗号化情報を復号化してＩＤ通知要求と乱数Ｒ１とに分離する。ここで、前記相互認証手段２１１は、分離した乱数Ｒ１と先に発生した乱数Ｒ１を比較し、両者が一致すれば充填端末１１が正当な処理（乱数Ｒ１の分離と合成および暗号化）を行った、つまり充填端末１１が支払カード２１と共通の暗号鍵を有する正当な充填端末であると認証し、受信したＩＤ通知要求に対する処理を行う。

【００５０】支払カード２１は、受信したＩＤ通知要求に対して、支払カード２１のカードＩＤ格納手段２１５に格納されているカードＩＤを支払カード２１の相互認証手段２１１で分離した乱数Ｒ２と合成して暗号化し、さらに前記相互認証手段２１１が発生した乱数Ｒ３とステータスＳ３を合成した合成情報として充填端末１１に送信する（ステップ５０３）。

【００５１】合成情報を受信した充填端末１１は、充填端末１１の相互認証手段１１１で受信した合成情報から乱数Ｒ３とステータスＳ３を分離して暗号化情報を取得し、この暗号化情報を復号化してカードＩＤと乱数Ｒ２とに分離する。前記相互認証手段１１１は、分離した乱数Ｒ２と先に発生した乱数Ｒ２を比較し、両者が一致すれば支払カード２１が正当な処理（乱数Ｒ２の分離と合成および暗号化）を行った、つまり支払カード２１が充填端末１１と共通の暗号鍵を有する正当な支払カードである認証し、受信したカードＩＤに対する処理を行う。

【００５２】充填端末１１は、受信したカードＩＤに基

づき、充填端末１１の発行残高管理手段１１４が発行残高管理データベース１３を参照して、支払カード２１に対する充填限度額を取得する。これは、１枚の支払カード、つまり１カードＩＤに対する価値の発行額を制限するもので、発行額の制限が必要ない場合には取得する必要はない。

【００５３】次に、充填端末１１が支払カード２１に対して充填限度額を通知するが、このときにも分離した乱数Ｒ３と充填限度額を合成して暗号化し、さらに発生した乱数Ｒ４とステータスＳ４を合成して送信し（ステップ５０４）、これを受信した支払カード２１が充填端末１１の認証を行うように、以下の通信では充填端末１１と支払カード２１はともに送信情報に分離した乱数を合成して暗号化し、さらに発生した乱数とステータスを合成して送信し、それを受信した側が認証を行うといった相互認証処理を通信毎に行うが認証方法は同様であるので以下では認証に関する説明は省略する。

【００５４】さて、充填限度額の通知を受けた支払カード２１は、その充填限度額の範囲内で価値の充填を受けるため、その充填額の減算要求を充填端末１１に送信する（ステップ５０５）。減算要求を受けた充填端末１１は、充填端末１１の価値充填手段１１２に格納されている価値を減算するとともに同額の加算要求を支払カード２１に対して送信し（ステップ５０６）、充填端末１１の発行残高管理手段１１４が発行残高管理データベース１３を更新する。

【００５５】加算要求を受けた支払カード２１は、支払カード２１の価値加減算手段２１２が価値格納手段２１３に格納されている価値に、加算要求の額を加算することで価値を充填し、充填終了を充填端末１１に通知する（ステップ５０７）。

【００５６】なお、通信中に認証が失敗した場合やステータスの番号が不順となった場合には、通信に異常が生じたものとして充填処理を中止するが、充填処理では充填端末１１側での減算処理の後に支払カード２１の加算処理を行うため、発行した価値が不正に増額することはない。

【００５７】図７（ｂ）は、取引の際に支払カード２１と取引端末３２と収納カード３１の間で授受されるデータの流れを示した図である。

【００５８】まず、支払カード２１と収納カード３１が取引端末３２に挿入され、支払カード２１の送／受信手段２１４と取引端末３２の送／受信手段３２１が接続され、収納カード３１の送／受信手段３１４と取引端末３２の送／受信手段３２２が接続されて支払カード２１と取引端末３２、収納カード３１と取引端末３２が通信可能な状態になると、販売者３が取引端末３２の図示しない入力手段から取引する価値の額を入力する。

【００５９】価値の額が入力されると、取引端末３２の取引開始通知手段３２３が支払カード２１に対して取引開始要求を送信する（ステップ５１１）。なお、この取引開始要求には取引する価値の額が含まれている。

【００６０】取引開始要求を受けた支払カード２１は、収納カード３１と通信を行って価値の移動を行うが、以下の通信には取引端末３２は介入せずに支払カード２１と収納カード３１の間でのみ通信が行われる。また、支払カード２１と収納カード３１は、通信を行う際には、その通信毎に支払カード２１の相互認証手段２１１と収納カード３１の相互認証手段３１１の動作により相互に認証を行うが、その認証方法は上述の充填処理で説明したのと同様であるので、ここでは説明は省略する。

【００６１】さて、取引開始要求を受けた支払カード２１は、取引要求を収納カード３１に送信する（ステップ５１２）。この取引要求には、取引する価値の額と支払カード２１のカードＩＤ格納手段２１５に格納されている支払カード２１に固有のカードＩＤが含まれている。

【００６２】次に、収納カード３１が取引額に応じた減算要求を支払カード２１に対して送信し（ステップ５１３）、これを受けた支払カード２１では、支払カード２１の価値加減算手段２１２が価値格納手段２１３に格納されている価値を減算するとともに、減算額（取引額）に応じた加算要求を収納カード３１に送信する（ステップ５１４）。

【００６３】加算要求を受けた収納カード３１では、収納カード３１の価値加減算手段３１２が価値格納手段３１２に格納されている価値に、加算要求で要求された取引額を加算する。このとき、価値格納手段３１２は、格納する価値を先に取得したカードＩＤと対応させて格納する。

【００６４】加算要求に対する処理が終了すると、収納カード３１は取引終了を支払カード２１に通知し、価値の移動（取引）処理を終了する（ステップ５１５）。

【００６５】また、取引端末３２は、支払カード２１と収納カード３１の通信に介入することはないが、その通信内容を傍受してステータスＳｎを取得することにより取引の進行状況を知ることができる。

【００６６】図７（ｃ）は、価値清算の際に収納カード３１と清算端末１２との間で授受されるデータの流れを示した図である。

【００６７】まず、収納カード３１が清算端末１２に挿入され、収納カード３１の送／受信手段３１４と清算端末１２の送／受信手段１２３が接続されて収納カード３１と清算端末１２が通信可能な状態になると、収納カード３１が清算する価値の額（通常は全額）を含んだ清算要求を清算端末１２に送信する（ステップ５２１）。このとき、収納カード３１は、暗号化した清算要求に収納カード３１の相互認証手段３１１で発生した乱数Ｒ１とステータスＳ１を合成して送信するが、これは上述の価値充填の際に説明した相互認証と同様に、前記相互認証手段３１１と清算端末１２の相互認証手段１２１が相互

認証を行うために使用するものであり、以下、通信毎に相互認証を行うがその認証方法は同様であるため、ここでは説明は省略する。

【００６８】次に、清算要求を受けた清算端末１２が収納カード３１に対して、収納カード３１が有する所有者ＩＤを通知するようＩＤ通知要求を送信し（ステップ５２２）、これを受けた収納カード３１が収納カード３１の所有者ＩＤ格納手段３１５に格納されている収納カード３１の所有者（販売者３）に固有の所有者ＩＤを清算端末１２に送信する（ステップ５２３）。

【００６９】所有者ＩＤを受けた清算端末１２は、清算額に応じた減算要求を収納カード３１に送信する（ステップ５２４）。

【００７０】減算要求を受けた収納カード３１では、収納カード３１の価値加減算手段３１２が減算要求に応じて価値格納手段３１３に格納されている価値を減算するとともに、清算端末１２に加算要求を送信する（ステップ５２５）。この加算要求には価値格納手段３１３に格納されていた（価値加減算手段３１２が減算した）価値に対応して記憶されていたカードＩＤ（価値発行時に発行先となった支払カードに固有のＩＤ）が含まれている。

【００７１】加算要求を受けた清算端末１２では、清算端末１２の価値格納手段１２２に加算要求に応じた価値を格納（加算）するとともに、清算端末１２の発行残高管理手段１２４が加算要求に含まれるカードＩＤとこれに対応した価値の額に基づいて発行残高管理データベース１３の記憶内容を更新し、収納カード３１に清算終了を通知して清算処理を終了する（ステップ５２６）。

【００７２】以上、価値の充填、取引、清算の際の価値の移動を説明したが、ここで、価値の流れと不正行為の検出について説明する。

【００７３】カード発行者１が発行する価値は、充填端末１１から使用者２の所有する支払カード２１に充填される。このとき、充填端末１１は充填した価値の額と充填先の支払カード２１のカードＩＤを対にして発行残高管理データベース１３に記録する。また、一度充填を行った支払カード２１にさらに価値を充填する際には、発行残高管理データベース１３を参照して、支払カード２１に対する価値の発行限度額の範囲内で充填を行い（発行限度額が設定されている場合のみ）、充填後は発行残高管理データベース１３の記録を更新する。

【００７４】使用者２が販売者３から商品またはサービスの提供を受けると、その対価として、支払カード２１から取引端末３２を介して収納カード３１へ価値を移動する。

【００７５】販売者３は、使用者２から受けとった価値を清算して現金化する際には、収納カード３１に格納されている価値をカード発行者１の清算端末１２へ移動させる。このとき、清算端末１２は、収納カード３１から移動された価値の価値額とこれに対応したカードＩＤ番号に基づいて発行残高管理データベース１３の記録を更新する。

【００７６】価値の充填、取引、清算の各過程では、上述のように価値の送り側と受け側とで相互認証を行いながら、送り側での価値の減額の後に受け側での価値の増額を行って価値を移動させているため、支払カード２１や収納カード３１を偽造することは困難であり、価値の移動中にカードを引き抜くなどの操作を行っても、価値を増額することはできない。

【００７７】また、仮にカードの偽造や価値の複製等が行われたとしても、カード発行者１は発行残高管理データベース１３の記録に基づいて、不正行為を検出することができる。

【００７８】図８は、不正行為の検出の流れを示すフローチャートである。発行残高管理データベース１３が動作を開始し（ステップ６０１）、充填または清算による価値の額に対する更新処理があった場合に（ステップ６０２でＹＥＳ）、その更新処理を行う価値と対応するカードＩＤに関する記録を検索し（ステップ６０３）、その記録（充填または清算価値額）を更新する（ステップ６０４）。

【００７９】記録の更新の結果、充填した価値額よりも清算した価値額の方が大きくなった場合には（ステップ６０５でＹＥＳ）、不正行為が行われたことを検出し（ステップ６０６）、不正検出処理を終了する（ステップ６０７）。

【００８０】不正が検出された場合には、清算時に取得した収納カード３１の所有者ＩＤと価値と対応するカードＩＤに基づいて追跡を行う。

【００８１】また、支払カード２１と収納カード３１の両者に価値の移動を行う毎に、その内容を履歴として記録するように構成しておけば、不正が生じた場合には、そのカードを不正の証拠とすることができる。

【００８２】なお、支払カード２１にカードＩＤを付さずに使用した場合にもセキュリティー上は所定の効果が得られ、カードＩＤを付した場合にもカードＩＤと使用者２の関係を登録する必要はないので使用者２のプライバシーを保つことは可能である。

【００８３】次に、この発明に係わるＩＣカードを用いた決済方法およびシステムの第２の実施例について説明する。

【００８４】この第２の実施例では、カード発行者が発行する価値に発行番号（識別番号）を付して発行し、この発行番号を利用することで発行した価値の管理や不正の検出を行う。

【００８５】この第２の実施例におけるシステムは、上述の第１の実施例と同様に、カード発行者１が有する充填端末１１と清算端末１２と発行残高管理データベース１３、使用者２が有する支払カード２１、販売者３が有

する収納カード３１と取引端末３２で構成される（図１参照）。

【００８６】また、システムを構成する各部も上述の第１の実施例とほぼ同様であるので異なる点のみを説明する。

【００８７】第２の実施例では、価値に付した発行番号を利用して発行した価値の管理や不正の検出を行うため、支払カード２１が該カードに固有のカードＩＤを格納する必要がなく、支払カード２１のカードＩＤ格納手段２１５を具備しない。また、充填端末１１の価値充填手段１１２と発行残高管理手段１１４、清算端末１２の価値格納手段１２２と発行残高管理手段１２４、支払カード２１の価値格納手段２１２、収納カード３１の価値格納手段３１２は、常に価値とその価値に付された発行番号を対応させて処理を行う。

【００８８】つまり、充填端末１１から発行された価値には必ず発行番号が付され、この発行番号は同一の時間に同一の支払カード２１へ発行する価値は同一の番号となるが、異なる時間や異なる支払カード２１に対して発行する価値には異なる発行番号となる。支払カード２１は、取引により収納カード３１に価値を移動する際には、価値とその価値の発行番号を対にして移動させる。このとき、取引により移動する価値の額が、充填端末１１より発行を受けた額よりも小さい場合には、価値が分割されるため、同一の発行番号を持つ価値が存在することになる。

【００８９】したがって、発行残高管理データベース１３は、清算された価値を発行番号毎に累積し、清算額が発行額を越えた価値が検出された場合にはそれを不正検出とする。

【００９０】なお、この第２の実施例においても価値の移動の際には、第１の実施例と同様に価値の送り側と受け側が相互に認証を行う。

【００９１】次に、この発明に係わるＩＣカードを用いた決済方法およびシステムの第３の実施例について説明する。

【００９２】この第３の実施例は、上述の第１の実施例および第２の実施例における支払カード２１と収納カード３１の両者を収支カードとして１枚のＩＣカードに具備したカードを利用する。

【００９３】図９は、収支カードの構成を示すブロック図である。収支カード４１は、相互認証手段４１１、価値加減算手段４１２、価値格納手段４１３、送／受信手段４１４、所有者ＩＤ格納手段４１５、カードＩＤ格納手段４１６を具備して構成される。相互認証手段４１１は、送／受信手段４１４を介して接続される充填端末１１や清算端末１２、支払カード２１、収納カード３１、他の収支カード４１とその正当性を相互に認証する手段であり、価値加減算手段４１２は、相互認証手段４１１により認証された相手との価値の移動のために価値格納手段４１３に格納されている価値の加算および減算を行う。

【００９４】この収支カード４１は、上述の各実施例における支払カード２１と収納カード３１の両者として使用でき、その動作は上述の実施例と同様なので説明は省略する。

【００９５】なお、収支カード４１が具備するカードＩＤ格納手段４１６は、上述の第２の実施例に対応させる場合には具備する必要はない。

【００９６】また、上述の各実施例で説明したように、支払カード２１（または収支カード４１）から収納カード３１（または収支カード４１）へ価値を移動させる際に、取引端末３２は両者の通信に介入しない。つまり、取引端末３２は各実施例における決済システムのセキュリティーには関与していない。

【００９７】したがって、支払カード２１（または収支カード４１）から収納カード３１（または収支カード４１）への価値の移動は、通信回線を介して行うこともできる。この通信回線は専用線や電話回線等の比較的セキュリティー性の高いものでも、インターネットのようにセキュリティー性の低いものでも利用できる。

【００９８】例えば、図１０（ａ）に示すように、インターネット５０に接続された端末５１－１乃至５１－６のいずれかの間で価値の移動を行うことができ、インターネット上でのオンラインショッピングの決済に利用することもできる。この場合の各端末５１－１乃至５１－６は、専用の端末でもパーソナル・コンピュータ等にＩＣカードリーダライタを接続してこれを端末として利用してもよい。

【００９９】また、図１０（ｂ）に示すように、収納カード３１（または収支カード４１）を挿入する端末６０に、支払カード２１（または収支カード４１）を挿入する複数の端末６１－１乃至６１－４を接続して価値の移動を行うことができる。この図１０（ｂ）に示すシステムは、例えば商店等において、端末６０を事務室に設置して端末６１－１乃至６１－４を夫々レジスタに配置することで売り上げの全てを１枚の収納カードに集約する場合等に利用できる。

【０１００】なお、上述の各実施例において、充填端末１１に現金収受機能や、口座引落機能、クレジット決済機能等を設け、清算端末１２に現金払出機能や口座振込機能等を設けることでより一層、利用範囲を広げることもできる。

【０１０１】

【発明の効果】以上説明したように、この発明によれば、使用者が身分を明かすことなく支払カードへの価値の充填および販売者との取引を行い、販売者は身分を明かして価値の清算を行い、支払カードと収納カードが相互認証を行って価値を移動させるように構成したので、使用者のプライバシーが保護できるとともに支払カード

の譲渡が可能となり、価値を移動させる際の取引端末はシステムの安全に関与しないため、通信を介したり広範囲に設置したりすることができる。また、偽造価値の使用等の不正に加え販売者の脱税等の不正を行うことも困難とすることができる。

【０１０２】また、支払カードに固有のＩＤや発行価値に固有の発行番号等を利用することで不正が生じた場合の追跡を容易に行うことができる。

【図面の簡単な説明】

【図１】ＩＣカードを用いた決済システムのシステム構成を示すブロック図。

【図２】充填端末の詳細を示すブロック図。

【図３】清算端末の詳細を示すブロック図。

【図４】支払カードの詳細を示すブロック図。

【図５】収納カードの詳細を示すブロック図。

【図６】取引端末の詳細を示すブロック図。

【図７】価値の充填、取引、清算の際の各々の通信データの流れを示した図。

【図８】不正行為の検出の流れを示すフローチャート。

【図９】収支カードの構成を示すブロック図。

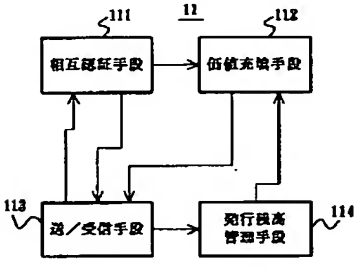
【図１０】決済システムの利用例を示した図。

【図１１】従来のシステムにおける流通過程でのＩＣカード内に格納されている価値の形態を示した図。

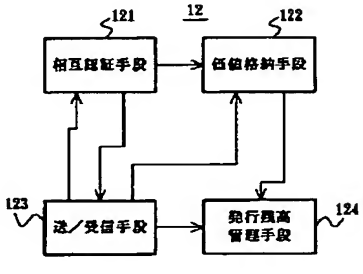
【符号の説明】

１　カード発行者
２　使用者
３　販売者
１１　充填端末
１２　清算端末
１３　発行残高管理データベース
２１　支払カード
３１　収納カード
３２　取引端末
＊４１　収支カード
５０　インターネット
５１－１～５１－６　端末
６０　端末
６１－１～６１－４　端末
１１１　相互認証手段
１１２　価値充填手段
１１３　送／受信手段
１１４　発行残高管理手段
１２１　相互認証手段
１２２　価値格納手段
１２３　送／受信手段
１２４　発行残高管理手段
２１１　相互認証手段
２１２　価値加減算手段
２１３　価値格納手段
２１４　送／受信手段
２１５　カードＩＤ格納手段
３１１　相互認証手段
３１２　価値加減算手段
３１３　価値格納手段
３１４　送／受信手段
３１５　所有者ＩＤ格納手段
３２１　送／受信手段
３２２　送／受信手段
３２３　取引開始通知手段
４１１　相互認証手段
４１２　価値加減算手段
４１３　価値格納手段
４１４　送／受信手段
４１５　所有者ＩＤ格納手段
４１６　カードＩＤ格納手段
＊

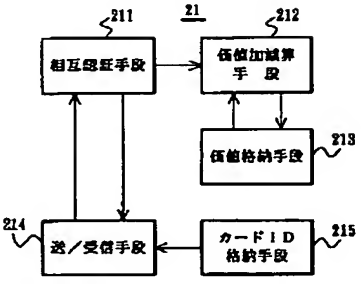
【図２】



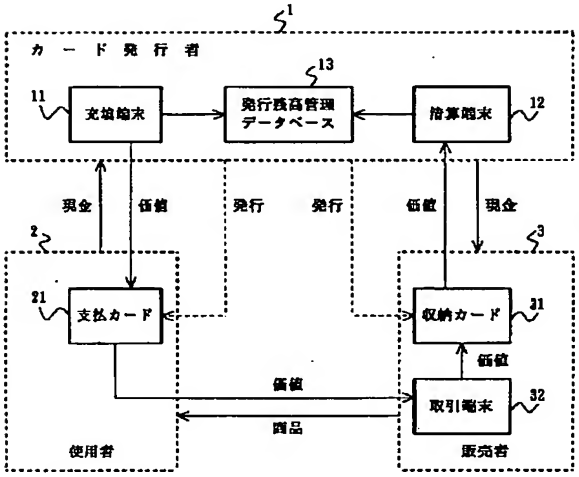
【図３】



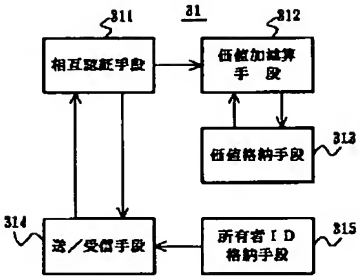
【図４】



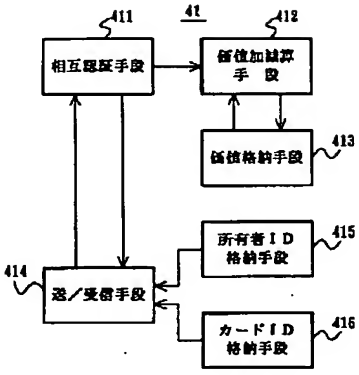
【図１】


カード発行者
1
11
充填端末
13
発行残高管理データベース
12
精算端末
現金
価値
発行
発行
価値
現金
2
3
21
支払カード
収納カード
31
価値
価値
32
取引端末
商品
使用者
販売者

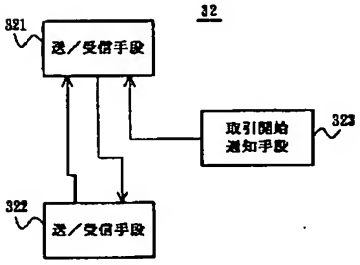
【図５】


311
31
312
相互認証手段
価値加減算手段
313
価値格納手段
314
送／受信手段
所有者ＩＤ格納手段
315

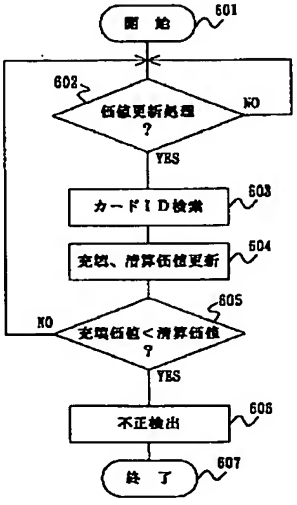
【図９】


411
41
412
相互認証手段
価値加減算手段
413
価値格納手段
所有者ＩＤ格納手段
415
414
送／受信手段
カードＩＤ格納手段
416

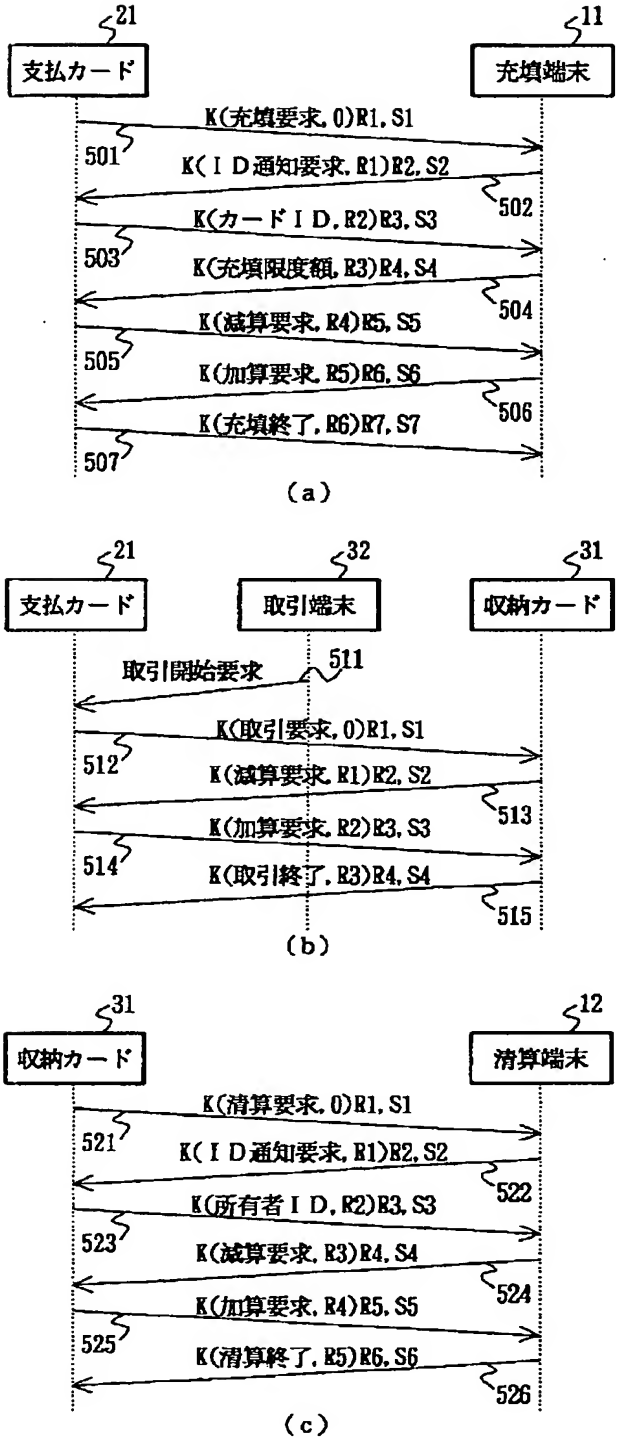
【図６】


32
321
送／受信手段
取引開始通知手段
323
322
送／受信手段

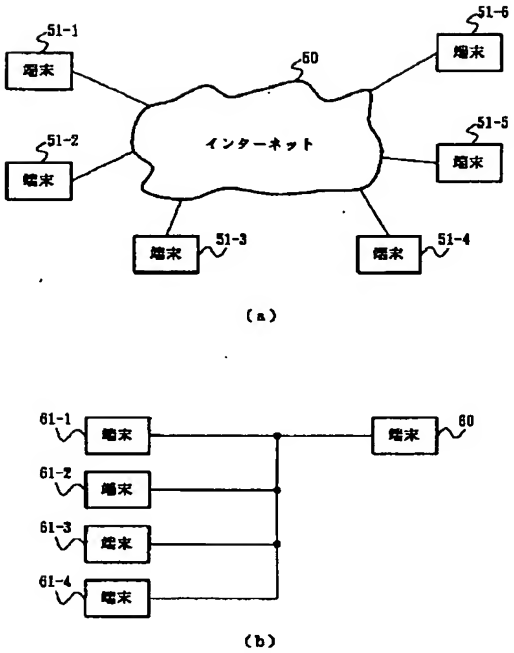
【図８】


開始
601
602
価値更新処理？
NO
YES
カードＩＤ検索
603
充填、精算価値更新
604
605
充填価値＜精算価値？
NO
YES
不正検出
606
終了
607

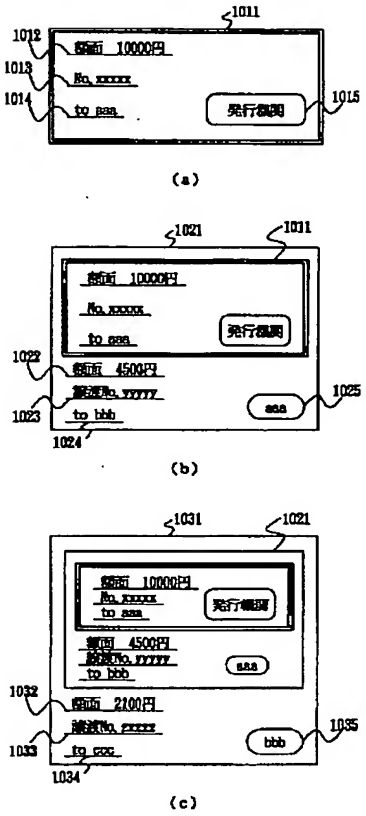
【図７】


21
支払カード
11
充填端末
K(充填要求,0)R1,S1
501
K(ＩＤ通知要求,R1)R2,S2
502
K(カードＩＤ,R2)R3,S3
503
K(充填限度額,R3)R4,S4
504
K(減算要求,R4)R5,S5
505
K(加算要求,R5)R6,S6
506
K(充填終了,R6)R7,S7
507
(a)
21
支払カード
32
取引端末
31
収納カード
取引開始要求
511
K(取引要求,0)R1,S1
512
K(減算要求,R1)R2,S2
513
K(加算要求,R2)R3,S3
514
K(取引終了,R3)R4,S4
515
(b)
31
収納カード
12
清算端末
K(清算要求,0)R1,S1
521
K(ＩＤ通知要求,R1)R2,S2
522
K(所有者ＩＤ,R2)R3,S3
523
K(減算要求,R3)R4,S4
524
K(加算要求,R4)R5,S5
525
K(清算終了,R5)R6,S6
526
(c)

【図１０】


51-1
端末
51-6
端末
50
インターネット
51-2
端末
51-5
端末
端末
51-3
端末
51-4
(a)
61-1
端末
端末
80
61-2
端末
61-3
端末
61-4
端末
(b)

【図１１】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
G07G	1/12	321	G06K	19/00	R
	1/14		G07F	7/08	Z

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.